CSO ASSIGNMENT 2

Gowlapalli Rohit

2021101113

Q3-Info about my Inspiron 15 3000 Laptop system

Operating System(OS):

```
Kernel           : Linux 5.14.0-1038-oem (x86_64)
C Library        : GNU C Library / (Ubuntu GLIBC 2.31-0ubuntu9.9) 2.31
Distribution     : Ubuntu 20.04.4 LTS(GNOME version: 3.36.8)
Computer Name    : rohit-Inspiron-15-3511
Language         : en_GB.UTF-8 (en_IN:en)(OS-Type: 64-bit)
Windowing System : X11
```

USB Devices

```
Linux Foundation 3.0 root hub
Microdia Integrated_Webcam_HD
Realtek Semiconductor Corp. Bluetooth Radio
Linux Foundation 2.0 root hub
```

Battery

```
Battery             : LI-Ion,3-cell, 41 Wh, lithium-polymer type battery
Capacity            : 32 / Normal (SMP manufactured)
Model Number        : DELL MGCM516(Serial Number = 5115)
Battery voltage     : 11.25 VDC (4 hrs charging time)
Battery Height x Width x depth      : 206.4 mm x 82 mm x 5.75 mm
Battery Temperature Range(Operating): 0°C to 35°C
```

PCI Devices

```
Host bridge                     : Intel Corporation Device 9a14 (rev 01)
VGA compatible controller: Intel Corporation Device 9a49(rev 01)(prog-if 00 [VGA controller])
Signal processing controller    : Intel Corporation Device 9a03,9a0d (rev 01)
RAID bus controller : Intel Corporation Volume Management Device NVMe RAID Controller
USB controller      : Intel Corporation Device a0ed (rev 20) (prog-if 30 [XHCI])
(RAM memory,PCI bridge)         : Intel Corporation Device (a0ef,(a0b1,a0bc)) (rev 20)
Serial bus controller [0c80]    : Intel Corporation Device a0e8,a0e9,a0a4 (rev 20)
(Communication,SATA) controller : Intel Corporation Device (a0e0,a0d3) (rev 20)
System peripheral               : Intel Corporation Device 09ab
(ISA bridge,Audio device,SMBus) : Intel Corporation Device (a082,a0c8,a0a3) (rev 20)
Network controller: Realtek Semiconductor RTL8821CE 802.11ac PCIe Network Adapter
Non-Volatile memory controller  : Sandisk Corp Device 5007 (rev 01)
```

Storage

```
Model           : ATA ST1000LM035-1RK1(SEAGATE) Disk (Revision--1002)
SCSI Controller : scsi0
HDD,SSD Storage : 1 TB,256 GB
```

DMI

```
Product     : Name--Inspiron 15 3511  Family--Inspiron Vendor--Dell Inc.
BIOS        : Vendor--Dell Inc.  Version--1.11.0
Board       : Name--0042CN  Vendor--Dell Inc  Version--A00
Chassis     : Vendor--Dell Inc.  Type--[10] Notebook
```

Sensors

```
../../BAT0/in0          Voltage 10.99V      Battery
../../nvme0/temp1       Temperature 33.85°C HDD
coretemp/temp1          Temperature 42.00°C CPU
coretemp/temp2          Temperature 39.00°C CPU
coretemp/temp3          Temperature 40.00°C CPU
coretemp/temp4          Temperature 41.00°C CPU
coretemp/temp5          Temperature 38.00°C CPU
thermal/thermal_zone2   Temperature 39.05°C CPU
thermal/thermal_zone0   Temperature 39.05°C CPU
thermal/thermal_zone3   Temperature 41.05°C CPU
thermal/thermal_zone1   Temperature 20.00°C CPU
thermal/thermal_zone4   Temperature 41.00°C CPU
```

Processor

```
Name                        : 11th Gen Intel Core i5-1135G7 @ 2.40GHz
Logical CPU Configuration   : 8x4200.00MHz (Device ID--0x9A49)(ISA-64 bit)
Processor wattage           : 15 W
(Cores,Threads )            : (4,8)
Max Turbo Frequency,Clock Speed     : 4.20 GHz, 2.40 GHz
Cache,Max Memory Size               : 8 MB Intel® Smart Cache, 64 GB
Bus Speed,Clocks            : 4 GT/s,400.00-4200.00 MHz 8x
Lithography                 : 10 nm SuperFin
Configurable TDP-(up,down) Base Frequency:(2.40 GHz(28 W),900 MHz(12 W))
Processor Graphics          : Intel® Iris® Xe Graphics
```

```
Graphics Max Dynamic Frequency      : 1.30 GHz
Graphics Output             : eDP 1.4b, MIPI-DSI 2.0, DP 1.4, HDMI 2.0b
Execution Units             : 80 (TJUNCTION: 100°C)
OpenCL* Support             : 3.0 (Sockets Supported: FCBGA1449)
# of Displays Supported,Max # of Memory Channels    : 4,2
Multi-Format Codec Engines,Max CPU Configuration    : 1,2
(Microprocessor,Chipset) PCIe Revision: (Gen 4,Gen 3)
Package Size                : 45.5x25
```

Memory

```
Memory : 7.5GiB (DDR4)
Memory slots,speed    : Two SODIMM slots,2666 MHz
(Max,Min) memory configuration  :(16,4) GB
Memory size per slot            : 4 GB, 8 GB, 16 GB
RAM             : 8 GB
```

File Systems

```
NAME        FSTYPE    LABEL         MOUNTPOINT
sda
├─sda1
├─sda2      BitLocker
└─sda3      ext4                      /home
nvme0n1
├─nvme0n1p1 vfat      ESP           /boot/efi
├─nvme0n1p2
├─nvme0n1p3 BitLocker
├─nvme0n1p4 ntfs      WINRETOOLS
├─nvme0n1p5 ntfs      Image
├─nvme0n1p6 ntfs      DELLSUPPORT
└─nvme0n1p7 ext4                       /
```

Benchmark scores

```
    BenchMarks    Score
CPU Fibonacci      0.57
CPU BlowFish       1.67
CPU Cryptohash   712.79
GPU Drawing     8658.25
FPU FFT            0.84
```

Kernel Modules

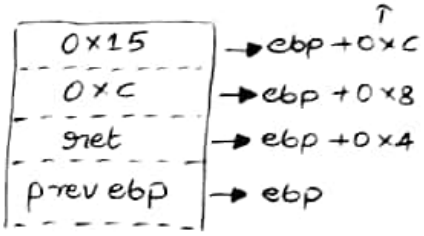
```
rfcomm              : Bluetooth RFCOMM ver 1.11
libcrc32c           : CRC32c (Castagnoli) calculations
br_netfilter        : Linux ethernet netfilter firewall bridge
llc                 : LLC IEEE 802.2 core support
cmac                : CMAC keyed hash algorithm
ecdh_generic        : ECDH generic algorithm
mc                  : Device node registration for media drivers
soundwire_intel     : Intel Soundwire Link Driver
soundwire_generic_allocation    : SoundWire Generic Bandwidth Allocation
snd_soc_acpi_intel_match        : Intel Common ACPI Match module
snd_hda_intel       : Intel HDA driver
snd_intel_dspcfg    : Intel DSP config driver
snd_intel_sdw_acpi  : Intel Soundwire ACPI helpers
snd_hwdep           : Hardware dependent layer
intel_tcc_cooling   : TCC offset cooling device Driver
x86_pkg_temp_thermal: X86 PKG TEMP Thermal Driver
snd_seq_midi        : Advanced Linux Sound Architecture sequencer MIDI synth.
dell_laptop         : Dell laptop driver
intel_powerclamp    : Package Level C-state Idle Injection for Intel CPUs
intel_rapl_msr      : Driver for Intel RAPL (Running Average Power Limit) control via MSR interface
snd_seq_midi_event  : MIDI byte &lt;-&gt; sequencer event coder
coretemp            : Intel Core temperature monitor
i915                : Intel Graphics
crct10dif_pclmul    : T10 DIF CRC calculation accelerated with PCLMULQDQ.
snd_rawmidi         : Midlevel RawMidi code for ALSA.
ghash_clmulni_intel : GHASH hash function, accelerated by PCLMULQDQ-NI
rtw88_pci           : Realtek 802.11ac wireless PCI driver
aesni_intel         : Rijndael (AES) Cipher Algorithm, Intel AES-NI instructions optimized
rtw88_core          : Realtek 802.11ac wireless core module
mac80211            : IEEE 802.11 subsystem
snd_seq             : Advanced Linux Sound Architecture sequencer.
dell_wmi            : Dell laptop WMI hotkeys driver
snd                 : Advanced Linux Sound Architecture driver for soundcards.
dell_smbios         : Common functions for kernel modules using Dell SMBIOS
input_leds          : Input -&gt; LEDs Bridge
dcdbas              : Dell Systems Management Base Driver (version 5.6.0-3.4)
mei_me              : Intel(R) Management Engine Interface
dell_wmi_descriptor : Dell WMI descriptor driver
intel_pmt_telemetry : Intel PMT Telemetry driver
intel_pmt_class     : Intel PMT Class driver
i2c_algo_bit        : I2C-Bus bit-banging algorithm
processor_thermal_device_pci_legacy : Processor Thermal Reporting Device Driver
mei     : Intel(R) Management Engine Interface
intel_rapl_common   : Intel Runtime Average Power Limit (RAPL) common code
sysimgblt           : 1-bit/8-bit to 1-32 bit color expansion (sys-to-sys)
igen6_edac          : MC Driver for Intel client SoC using In-Band ECC
int3403_thermal     : ACPI INT3403 thermal driver
int340x_thermal_zone: Intel INT340x common thermal zone handler
int3400_thermal     : INT3400 Thermal driver
acpi_thermal_rel    : Intel acpi thermal rel misc dev driver
i2c_i801            : I801 SMBus driver
intel_lpss_pci      : Intel LPSS PCI driver
intel_lpss          : Intel LPSS core driver
intel_pmt           : Intel Platform Monitoring Technology PMT driver
pinctrl_tigerlake   : Intel Tiger Lake PCH pinctrl/GPIO driver
```

Q4) Given that assemblycode (a,b) implies
push b
push a → Process-①
call assemblycode

In lines <+18> and <+38>, it is assumed that "assembly code" should be present in place of "asm2"

In Q4, assemblycode (0xc, 0x15) is called
push 0x15
push 0xc
call assemblycode

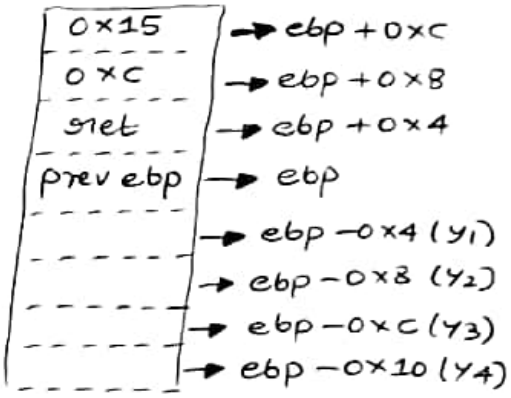
Stack-Status (12)10



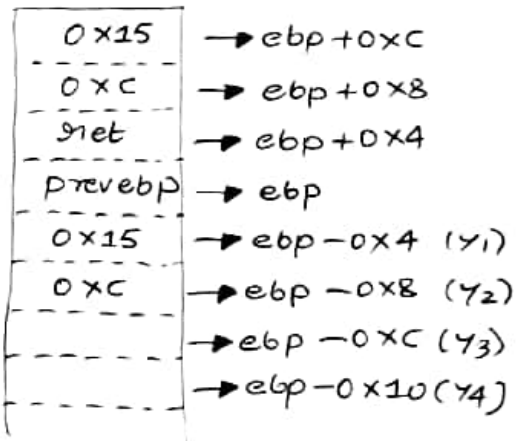
<+0>: push ebp # push ebp onto stack
<+1>: mov ebp,esp # copy esp to ebp
<+3>: sub esp,0x10 → (16)10 # reserving 16 bytes on stack

esp register is an indicator for the top of the stack, it changes/grows as stack grows/shrinks

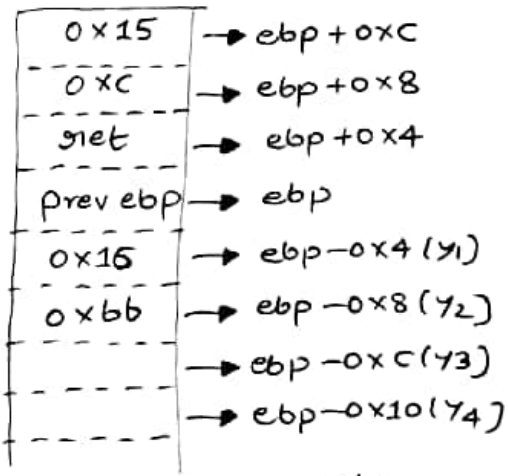
ebp is helping register, we push content of ebp on stack, then we copy esp to ebp, that is why when we refer to other items on stack, we use constant value of ebp (not changing value of esp), (y_1, y_2, y_3, y_4 are local variables)



<+6>: mov eax, DWORD PTR [ebp+0xc]
eax = 0x15
<+9>: mov DWORD PTR [ebp-0x4], eax
y_1 = 0x15
<+12>: mov eax, DWORD PTR [ebp+0x8]
eax = 0xc
<+15>: mov DWORD PTR [ebp-0x8], eax
y_2 = 0xc
<+18>: jmp 0x50c <assemblycode+31>
jumps to <+31> like below



<+20>: add DWORD PTR [ebp-0x4], 0x1
y_1 = 0x15+0x1 = 0x16
<+24>: add DWORD PTR [ebp-0x8], 0xaf
y_2 = 0xc+0xaf = 0xbb
<+31>: cmp DWORD PTR [ebp-0x8], 0xa3d3
compares y_2 and 0xa3d3
<+38>: jle 0x501 <assemblycode+20>
jumps if y_2 <= 0xa3d3



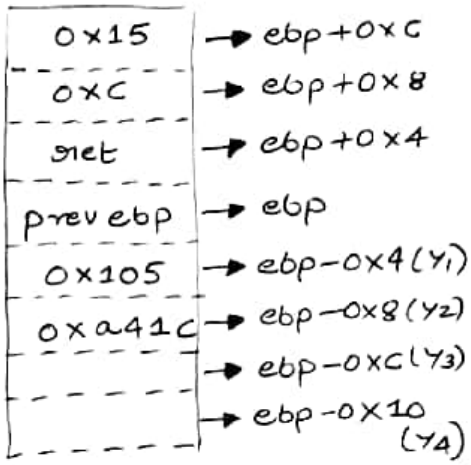
↳ when we enter the loop

The loop in the above block of code runs until y_2 > 0xa3d3, which would take $\frac{<0xa3d3>}{af} = \frac{41939}{175} \approx 240$ iterations

* It implies that we add 1 to 0x15, 240 times $\Rightarrow y_1 = 0x15 + 0xf0$
$= 0x105$

Stack-status at the end of loop

Stack-status



<+40>: mov eax, DWORD PTR [ebp-0x4]
eax = 0x105

The 4 bytes at [ebp-0x4] are moved to eax register. Arithmetic opcodes cannot operate with two memory-operands. Data needs to be moved to a register first before the arithmetic is performed, eax now holds the value of y_1 variable

<+43>: leave

Cleanup stack (reverse the "mov ebp, esp" from above. Destroys the stack frame, Essentially maps to pop ebp and restores the old stack-base pointer

<+44>: ret
Pops the top of stack treating the value as a return address and sets the program pointer (eip) to this value. The return address typically holds the address of the instruction directly after the call instruction that brought execution to this function

#assemblycode(0xc, 0x15) returns value of 0x105

```
assemblycode(int x1, int x2)
{
    int c = x2; //ebp-0x4
    int d = x1; //ebp-0x8
  while(d<=0xa3d3)
   {
      c = c+(0x1);
      d = d+(0xaf);
   }
  return c;
}
```

equivalent C-code

Q5 (a) `gcc q5.c → ./a.out` → prints string

`./q5.out` → No such file/directory

Interpreter (1)

Interpreter for a.out = ./libc6-amd64-2.27-3ubuntu1-i386.ld

Interpreter for q5.out = /lib64/ld-linux-x86-64.so.2

After Interpreter for q5.out is changed to Interpreter-(1) and executed it prints string. Dynamic binaries need external components to run correctly. Different Interpreters need different external components for corresponding dynamic binary (DYN - shared object file). Interpreters translates program one-statement at a time. Often external components are normal libraries → (common functions)

Q5

(b) The binary file uses 64-bit architecture. It follows little-endian byte ordering. It is a shared object file (DYN). The expected machine type for this file is AMD x-86-64. (UNIX-System V) ABI is used (to understand overlap in common functions)