**Name:** Manish Lokhande **Student ID:** 014501344

**Name:** Pankaj Patil **Student ID:** 014535040

**Question 1**: For each member in your team, provide 1 paragraph detailing what parts of the lab that member implemented / researched.

**Answer:**

1. Work done by Manish Lokhande:

* Created leaf node %eax= 0x4FFFFFFE for **case II**
* Made required changes in cpuid.c and vmx.c
* Installed cupid Pakage on inner VM
* Tested and Verified results
* Documented the steps and results.

2. Work done by Pankaj Patil:

* Created leaf node %eax= 0x4FFFFFFC for **case IV**
* Made required changes in cpuid.c and vmx.c
* Tested and Verified results
* Documented the steps and results.

**Question 2**: Describe in detail the steps you used to complete the assignment.

**Answer:**

**Prerequisites:**

* Need a working assignment 1 configuration.

Verified: Assignment I code is functional.

**Step 1:** Add code to KVM at file **/linux/arch/x86/kvm/vmx/vmx.c** and

**/linux/arch/x86/kvm/cpuid.c**

1. For CPUID leaf node %eax= 0x4FFFFFFE:

Return the high 32 bits of the total time spent processing all exits in %ebx

Return the low 32 bits of the total time spent processing all exits in %ecx

%ebx and %ecx return values are measured in processor cycles, across **all** VCPUs.

1. For CPUID leaf node %eax= 0x4FFFFFFC:

Return the time spent processing the exit number provided (on input) in %ecx.

Return the high 32 bits of the total time spent processing all exits in %ebx

Return the low 32 bits of the total time spent processing all exits in %ecx

* Below is the code which we modified in vmx.c to test the above functionality:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Below is the code which we modified in cpuid.c to test the above functionality:

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Step 2:** Build the updated code:

* **make modules**
* **make modules\_install**
* **make install**
* **Reboot**

**Step 3:** Open virt-manager and start virtual machine. Install CPUID package inside the inner vm.

* **sudo apt-get install cupid**

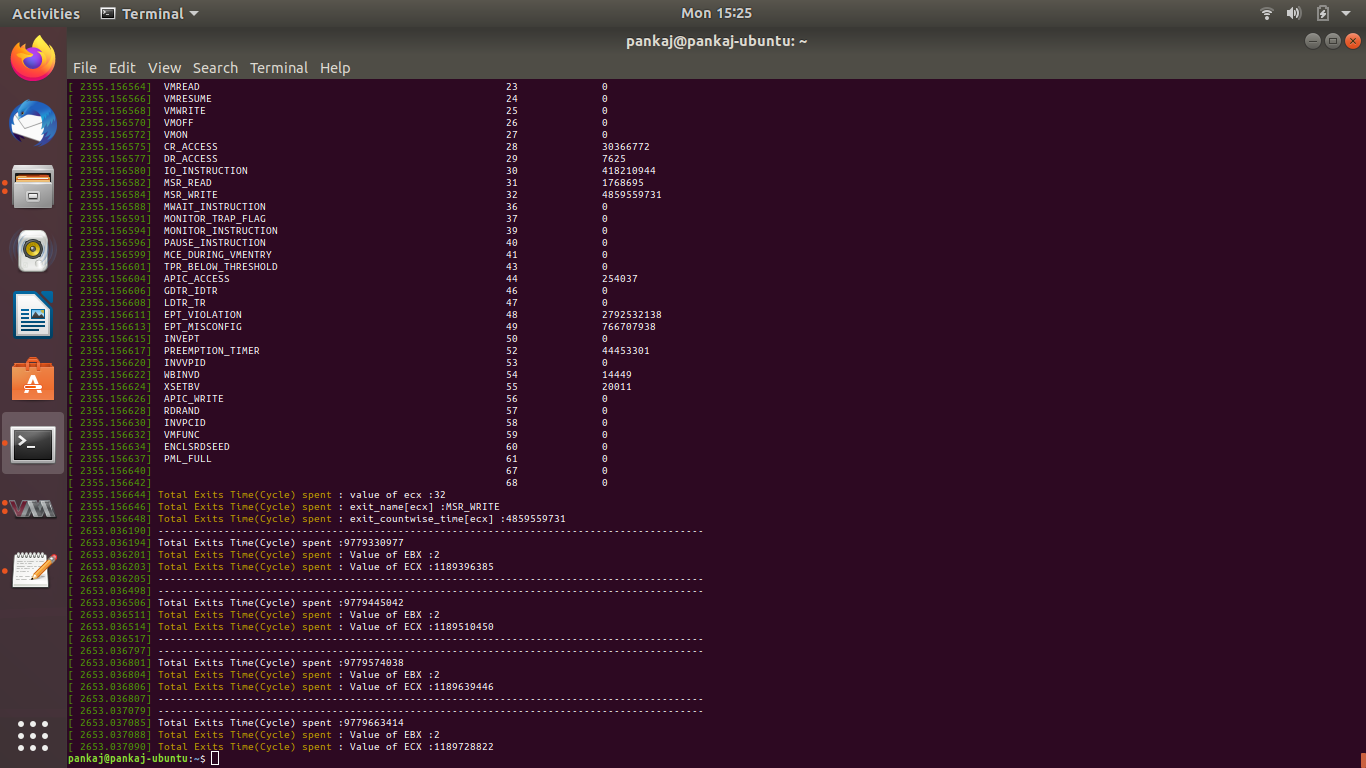
**Step 4:** Test the code using below commands for case 2:

1. cpuid -l 0x4FFFFFFE

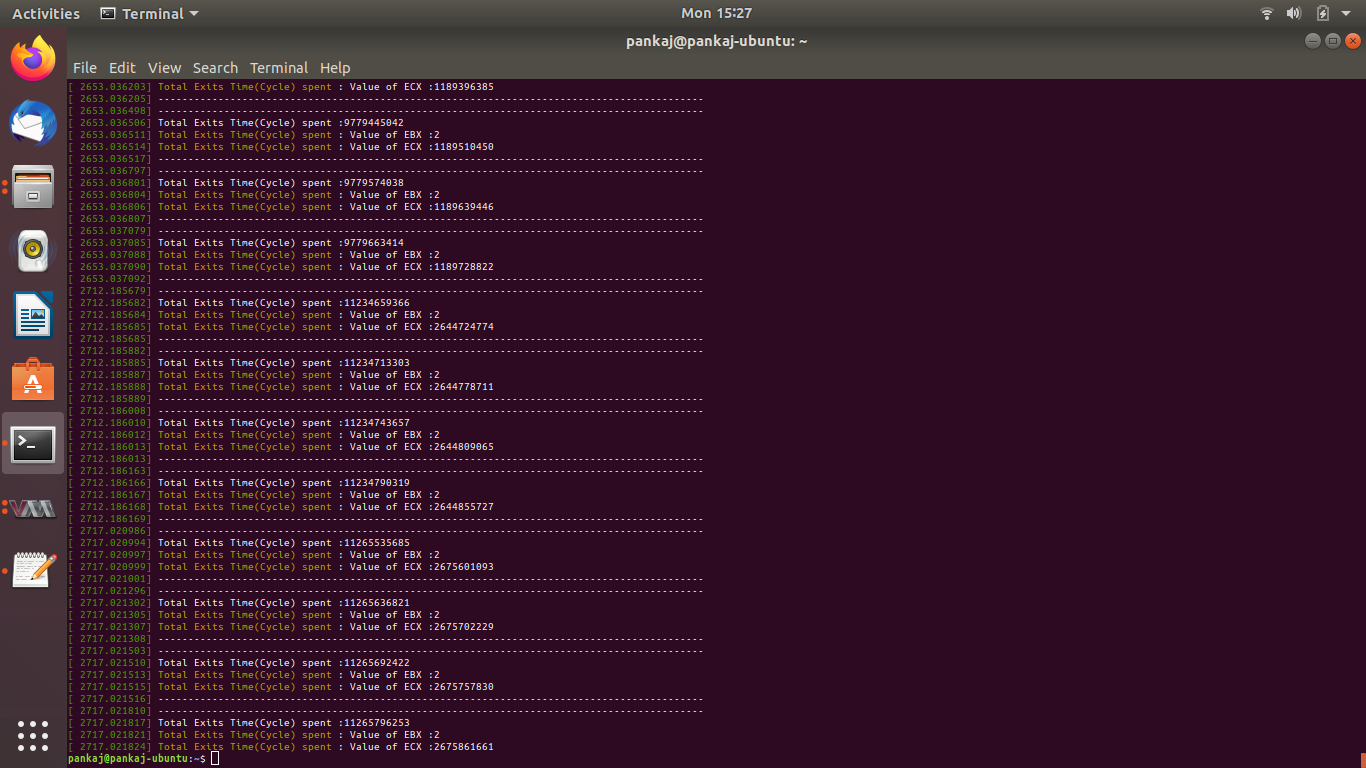
A screenshot of a computer

Description automatically generated

1. Try **dmesg** command in the host system’s terminal



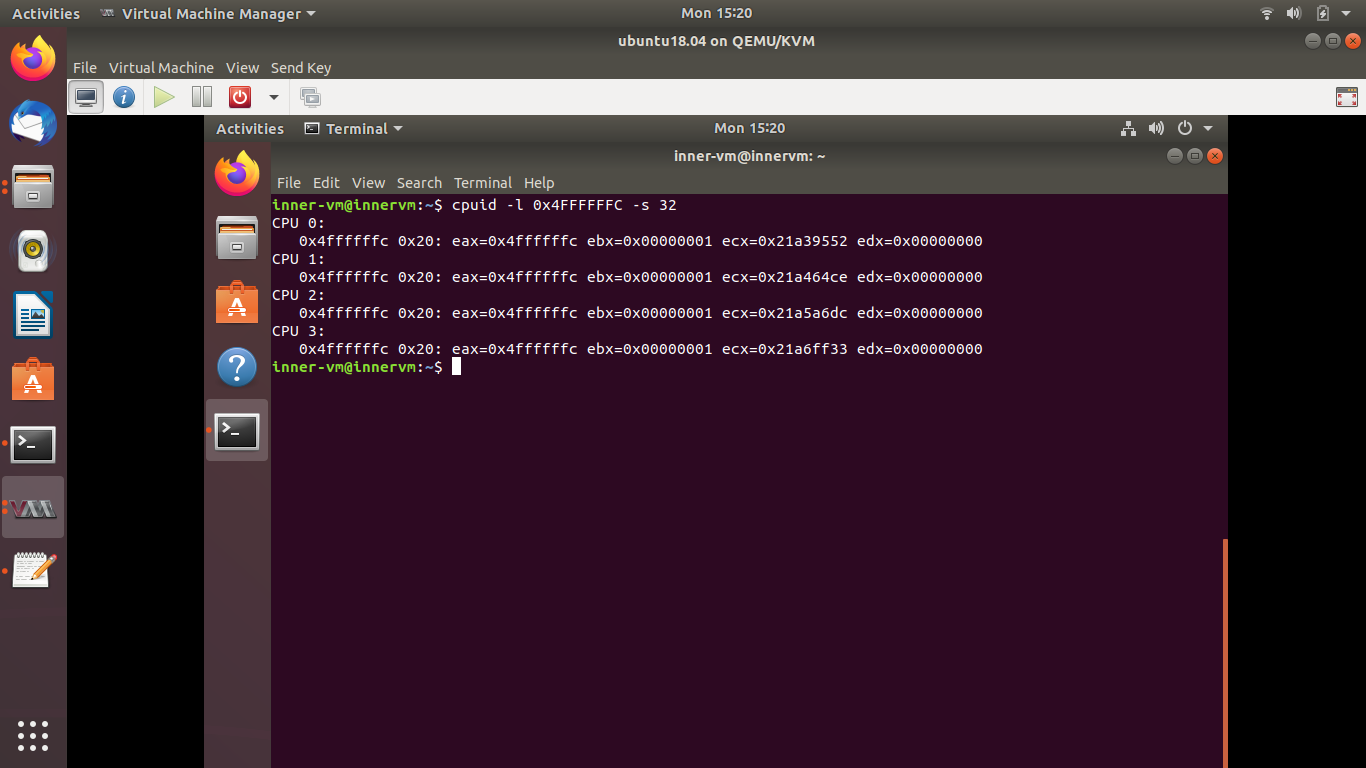
Total Exit count after rebooting



Total exits taken for VM reboot: 1486132839

**Step 5:** Test the code using below commands for case 4:

1. cpuid -l 0x4FFFFFFC s -32



1. Try **dmesg** command in the host system’s terminal to view count of all available exits.

**A screenshot of a computer

Description automatically generated**

1. Cupid -l 0x4FFFFFFC s -444 to test the output for invalid exit code.

**A screenshot of a computer screen

Description automatically generated**

1. cupid -l 0x4FFFFFFC s -3 to test the output for valid exit but not implemented by KVM.

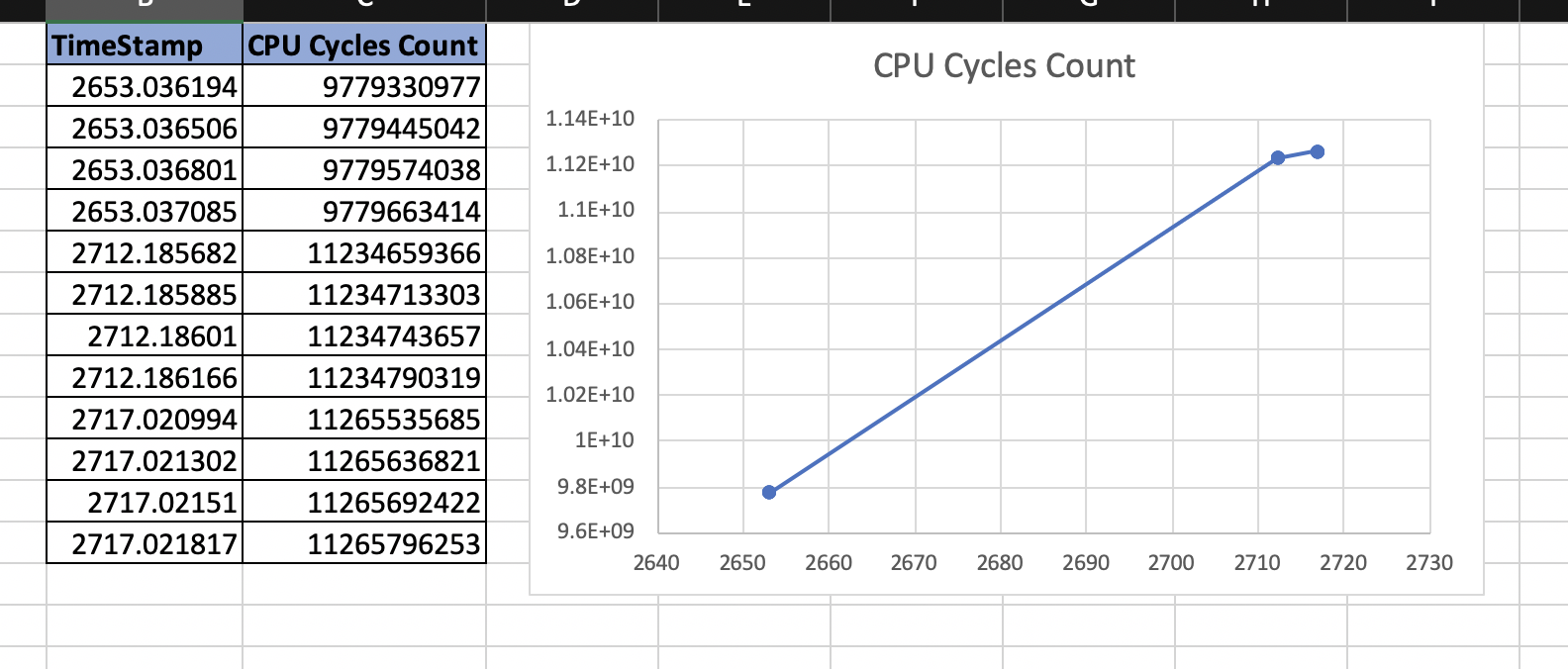
**A screenshot of a computer screen

Description automatically generated**

**Question 3**: Comment of the frequency of exits

**Answer:**

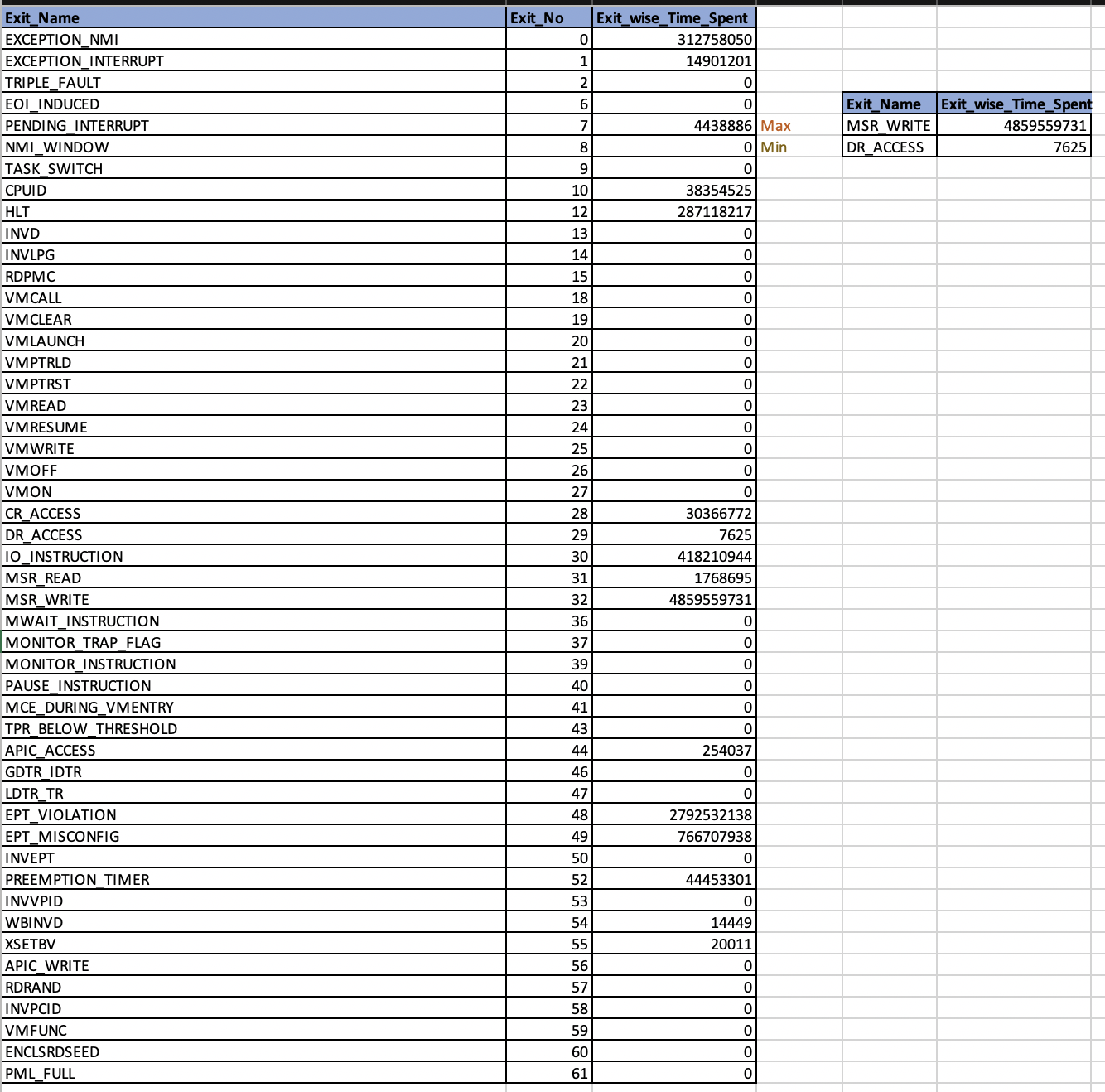
* Frequency of the time spent on exits are dependent on type of exit. If the system performs the more privileged operations, then the number of exits increases (i.e time spent on exits increases).

****

**Question 4**: Exit types defined in SDM, which are the most frequent and least frequent wrt Time spent?

**Answer:**

* Most frequent exit is MSR\_WRITE with Cycle Count 4859559731
* Least frequent exit is DR\_ACCESS with Cycle Count 7625 (non-zero)

****

**Github repo name**: linux

**Github username** : Manish0112

**URL**: <https://github.com/Manish0112/linux>

References:

Retrieved from https://www.cyberciti.biz/tips/compiling-linux-kernel-26.html

Retrieved from <https://www.linux.com/tutorials/how-compile-linux-kernel-0/>

Retrieved from <https://stackoverflow.com/questions/23402701/function-asm-volatile-rdtsc>

Retrieved from <https://www.youtube.com/watch?v=17UKKdHKMOE&t=1361s>