1.For each member in your team, provide 1 paragraph detailing what parts of the lab that member implemented / researched. (You may skip this question if you are doing the lab by yourself).

Radhika I has tried it multiple times on virtual machine VMWARE workstation, then did a dual boot and still faced some issues. Hence finally, removed all other OS and installed linux 17.04 and built the kernel from source. I have researched about the cupid function and helped to modify the code for cupid.c and create the test file to test the change in vendor string.

Shweta I has tried multiple times in my Macbook with VMWARE Fusion, but faced different types of errors. Then I researched about cupid function and changed the cupid.c and created the test file to test the change in the vendor string. I have helped to set up the system and I modified the test file and cupid.c file.

In the end, we both were able to run the functionality on a ubuntu machine - 4.14.0-rc+ kernel version. And ubuntu 17.

2.Describe in detail the steps you used to complete the assignment. Consider your reader to be someone skilled in software development but otherwise unfamiliar with the assignment. Good answers to this question will be recipes that someone can follow to reproduce your development steps. Note: I may decide to follow these instructions for random assignments, so you should make sure they are accurate.

Create live Ubuntu in USB and install Ubuntu Install Git:

```
sudo apt-get update sudo apt-get install git fakeroot build-essential ncurses-dev xz-utils libssl-dev bc
```

Check version of current linux kernel

```
Uname – r
```

Clone the Git repository for the latest linux kernel source code :

```
Git clone https://github.com/torvalds/linux.git
```

Note the COMMIT id

```
Git log
```

[Note the first commit id, which will be of the form as below:

Change to the Linux folder and configure the modules to be included/excluded

```
make menuconfig
```

Compile the kernel and its modules by checking number of processing units available

```
nproc [ to know the number of processing units, in our case it was 1] sudo make -j 1 && sudo make modules_install -j 1 && sudo make install -j 1
```

Once the kernel is built, use the following command to automatically look for the /boot folder and adds them to the grub’ s config file

```
update-grub
```

Check version now so that it shows the latest kernel version

Uname －r Change function kvm_emulate_cpuid function cupid.c file in /Linux/arch/x86/kvm/cupid.c to implement the assignment functionality. Once the changes have been done save the file and do the below commands

```
sudo make -j 4 && sudo make modules_install -j 4 && sudo make install -j 4
```

rmmod kvm_intel.ko Rmmod kvm.ko Insmod kvm.ko Insmod kvm-intel.ko Next install virt manager sudo apt install virt-manager Create new virtual machine using Ubuntu iso image in virt-manager. If this gives an error of failure-daemon, the below commands should be executed:

```
/etc/init.d/apparmor stop
update-rc.d apparmor remove
apt remove libvirtd
apt remove libvirt
apt remove virt-manager
apt remove libvirt-bin
apt-get install virt-manager
```

and reboot

Now Installing Ubuntu using iso image. This is the testvm.

Open command prompt and type CPUID, If this gives an error, sudo apt-get install cpuid

This will give a whole list of cupid features of which the first one is the vendor string, which will display GENUINE INTEL.

Write a test file to toggle the flag for checking the cupid functionality for toggled input.

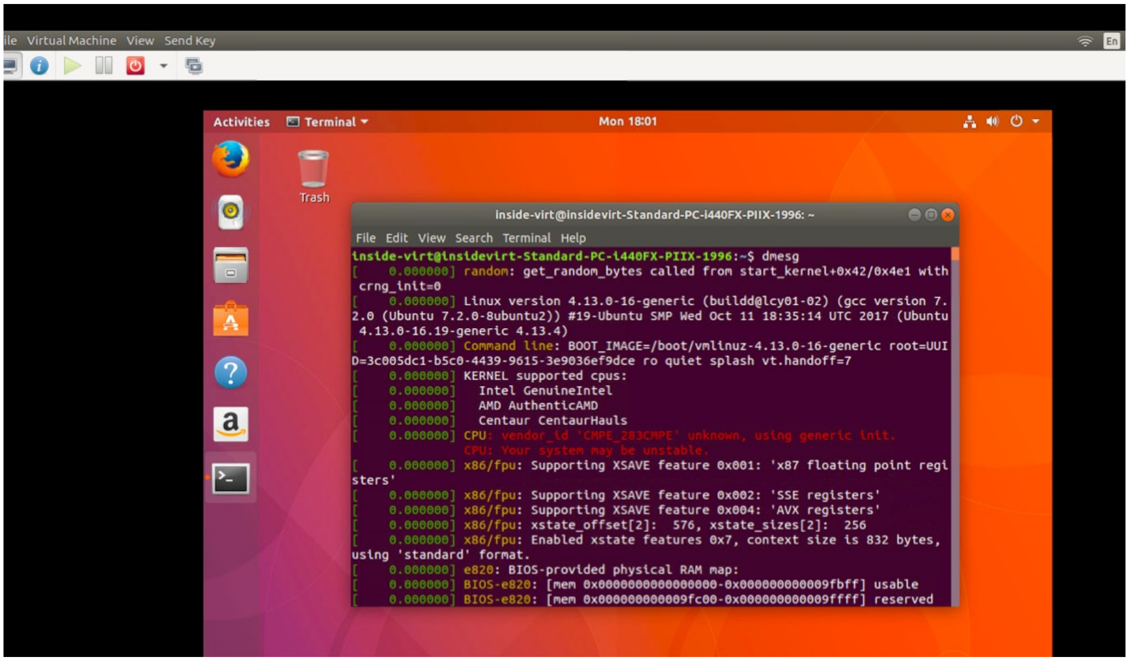
Executing this in the testvm will give changed vendor string as output.

For the third question in the assignment, clone the testvm to create another virtual machine.

Then, toggle the functionality in the testvm so that the string CMPE_283CMPE is displayed for vendor string in test vm. Once this is done, open the cloned vm and check cpuinfo using dmesg.

You will notice that for vendor string for is displayed as “CMPE_283CMPE” UNKNOWN...

3. With the assignment functionality enabled, boot a second linux VM (this can just be a plain linux VM or a copy of your test VM).
◦ What happens during boot? (Hint: check dmesg output).
During the boot, upon dmesg in the command line, the CPU details are mentioned, for which the vendor details are mentioned as ‘CMPE_283CMPE’ unknown and displays that my system may be unstable.

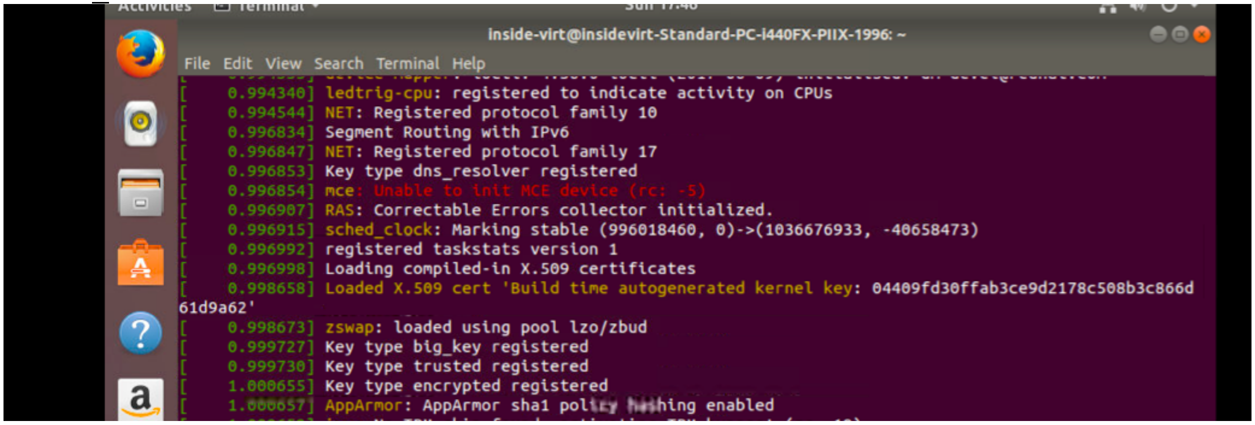


ile Virtual Machine View Send Key
Activities
Terminal
Mon 18:01
Trash
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help

```
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996:~$ dmesg
[    0.000000] random: get_random_bytes called from start_kernel+0x42/0x4e1 with
 crng_init=0
[    0.000000] Linux version 4.13.0-16-generic (buildd@lcy01-02) (gcc version 7.
2.0 (Ubuntu 7.2.0-8ubuntu2)) #19-Ubuntu SMP Wed Oct 11 18:35:14 UTC 2017 (Ubuntu
 4.13.0-16.19-generic 4.13.4)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-4.13.0-16-generic root=UUI
D=3c005dc1-b5c0-4439-9615-3e9036ef9dce ro quiet splash vt.handoff=7
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Centaur CentaurHauls
[    0.000000] CPU: vendor_id 'CMPE_283CMPE' unknown, using generic init.
               CPU: Your system may be unstable.
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regi
sters'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using 'standard' format.
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
```

◦ **Does the system behave differently?**

No, the system does not behave differently. Just the results of the dmesg indicate that the vendor_id is unknown

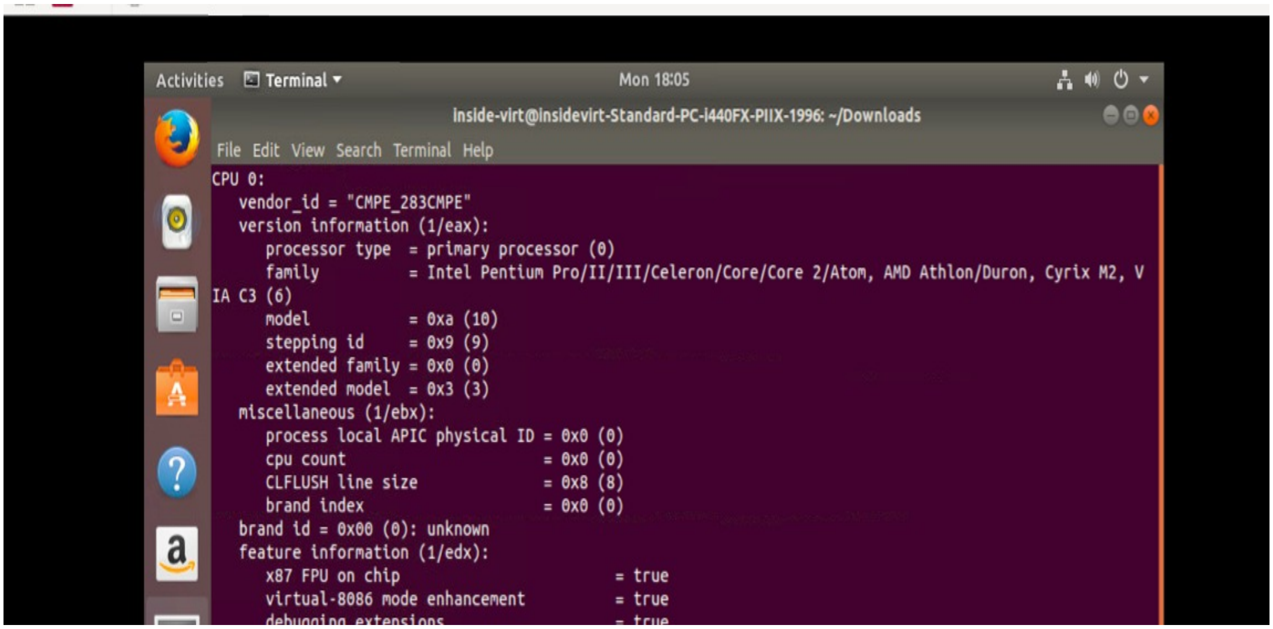


inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help

```
[    0.994340] ledtrig-cpu: registered to indicate activity on CPUs
[    0.994544] NET: Registered protocol family 10
[    0.996834] Segment Routing with IPv6
[    0.996847] NET: Registered protocol family 17
[    0.996853] Key type dns_resolver registered
[    0.996854] mce: Unable to init MCE device (rc: -5)
[    0.996907] RAS: Correctable Errors collector initialized.
[    0.996915] sched_clock: Marking stable (996018460, 0)->(1036676933, -40658473)
[    0.996992] registered taskstats version 1
[    0.996998] Loading compiled-in X.509 certificates
[    0.998658] Loaded X.509 cert 'Build time autogenerated kernel key: 04409fd30ffab3ce9d2178c508b3c866d
61d9a62'
[    0.998673] zswap: loaded using pool lzo/zbud
[    0.999727] Key type big_key registered
[    0.999730] Key type trusted registered
[    1.000655] Key type encrypted registered
[    1.000657] AppArmor: AppArmor sha1 policy hashing enabled
```

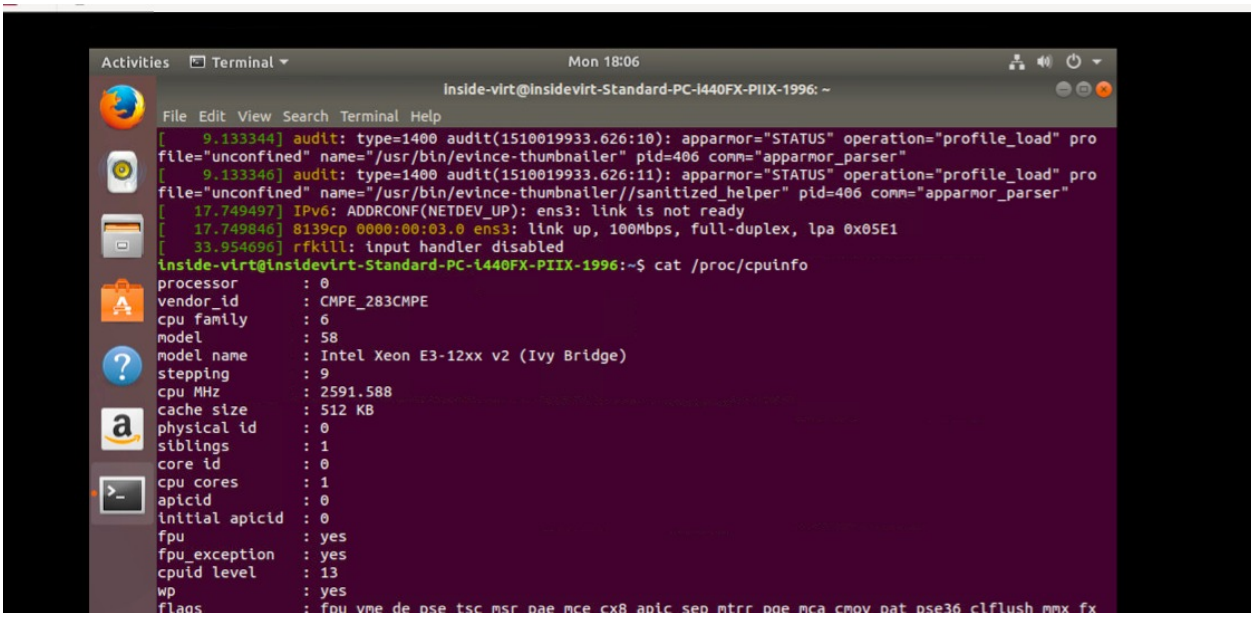
◦ **Does the content of /proc/cpuinfo change when the functionality is enabled vs disabled?**

Yes, the content changes based on the functionality being enabled or disabled.
If enabled, it displays CMPE_283CMPE and if disabled, it displays GenuineIntel



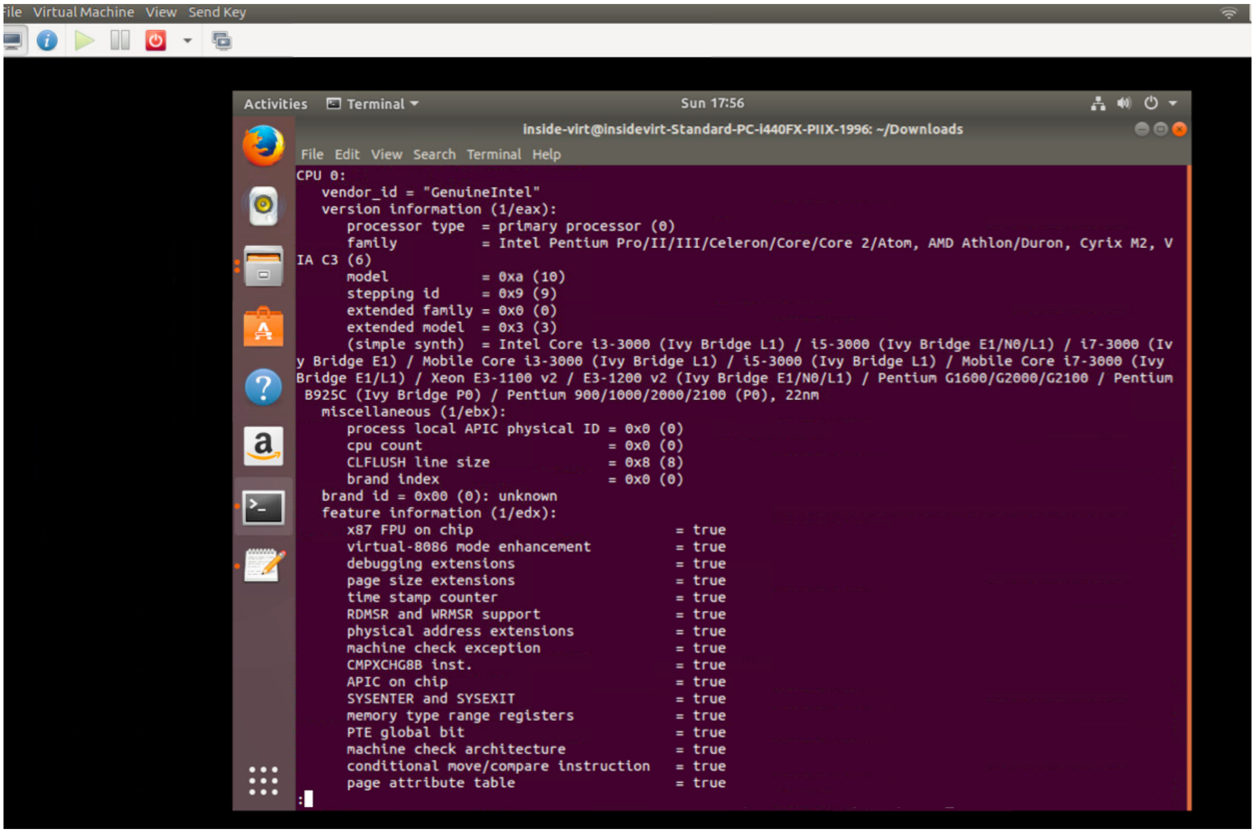
Activities
Terminal
Mon 18:05
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996: ~/Downloads
File Edit View Search Terminal Help

```
CPU 0:
   vendor_id = "CMPE_283CMPE"
   version information (1/eax):
      processor type  = primary processor (0)
      family          = Intel Pentium Pro/II/III/Celeron/Core/Core 2/Atom, AMD Athlon/Duron, Cyrix M2, V
IA C3 (6)
      model           = 0xa (10)
      stepping id     = 0x9 (9)
      extended family = 0x0 (0)
      extended model  = 0x3 (3)
   miscellaneous (1/ebx):
      process local APIC physical ID = 0x0 (0)
      cpu count                      = 0x0 (0)
      CLFLUSH line size              = 0x8 (8)
      brand index                    = 0x0 (0)
   brand id = 0x00 (0): unknown
   feature information (1/edx):
      x87 FPU on chip                        = true
      virtual-8086 mode enhancement          = true
      debugging extensions                   = true
```



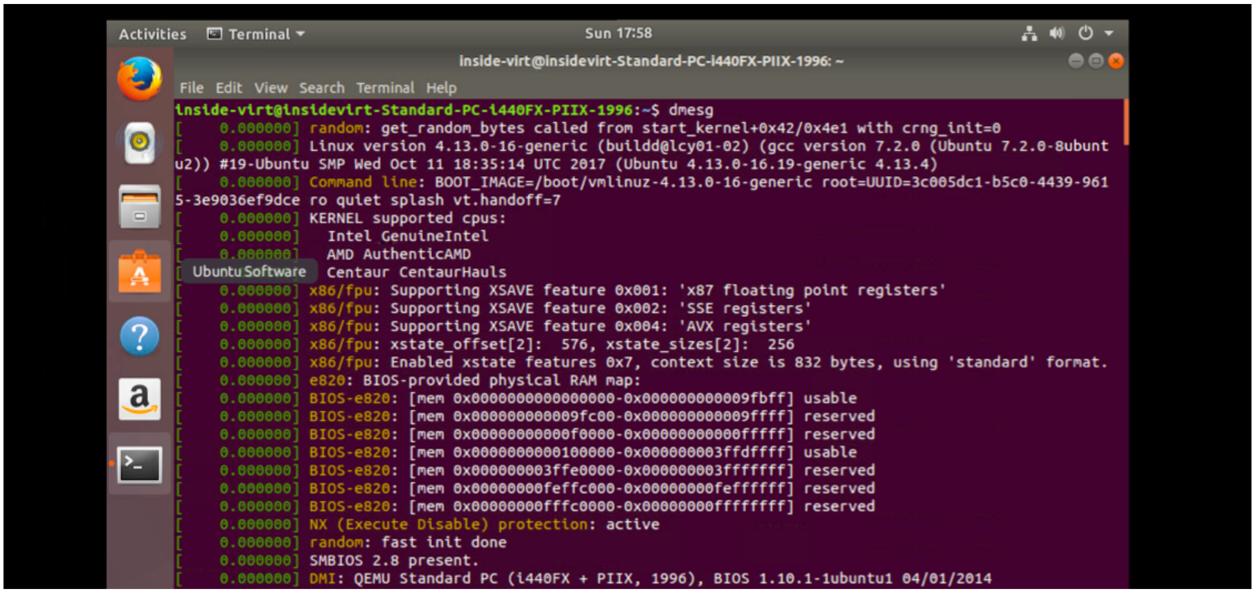
Activities
Terminal
Mon 18:06
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help

```
[    9.133344] audit: type=1400 audit(1510019933.626:10): apparmor="STATUS" operation="profile_load" pro
file="unconfined" name="/usr/bin/evince-thumbnailer" pid=406 comm="apparmor_parser"
[    9.133346] audit: type=1400 audit(1510019933.626:11): apparmor="STATUS" operation="profile_load" pro
file="unconfined" name="/usr/bin/evince-thumbnailer//sanitized_helper" pid=406 comm="apparmor_parser"
[   17.749497] IPv6: ADDRCONF(NETDEV_UP): ens3: link is not ready
[   17.749846] 8139cp 0000:00:03.0 ens3: link up, 100Mbps, full-duplex, lpa 0x05E1
[   33.954696] rfkill: input handler disabled
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996:~$ cat /proc/cpuinfo
processor       : 0
vendor_id       : CMPE_283CMPE
cpu family      : 6
model           : 58
model name      : Intel Xeon E3-12xx v2 (Ivy Bridge)
stepping        : 9
cpu MHz         : 2591.588
cache size      : 512 KB
physical id     : 0
siblings        : 1
core id         : 0
cpu cores       : 1
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fx
```


File Virtual Machine View Send Key
Activities
Terminal
Sun 17:56
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996: ~/Downloads
File Edit View Search Terminal Help

```
CPU 0:
   vendor_id = "GenuineIntel"
   version information (1/eax):
      processor type  = primary processor (0)
      family          = Intel Pentium Pro/II/III/Celeron/Core/Core 2/Atom, AMD Athlon/Duron, Cyrix M2, V
IA C3 (6)
      model           = 0xa (10)
      stepping id     = 0x9 (9)
      extended family = 0x0 (0)
      extended model  = 0x3 (3)
      (simple synth)  = Intel Core i3-3000 (Ivy Bridge L1) / i5-3000 (Ivy Bridge E1/N0/L1) / i7-3000 (Iv
y Bridge E1) / Mobile Core i3-3000 (Ivy Bridge L1) / i5-3000 (Ivy Bridge L1) / Mobile Core i7-3000 (Ivy
Bridge E1/L1) / Xeon E3-1100 v2 / E3-1200 v2 (Ivy Bridge E1/N0/L1) / Pentium G1600/G2000/G2100 / Pentium
 B925C (Ivy Bridge P0) / Pentium 900/1000/2000/2100 (P0), 22nm
   miscellaneous (1/ebx):
      process local APIC physical ID = 0x0 (0)
      cpu count                      = 0x0 (0)
      CLFLUSH line size              = 0x8 (8)
      brand index                    = 0x0 (0)
   brand id = 0x00 (0): unknown
   feature information (1/edx):
      x87 FPU on chip                        = true
      virtual-8086 mode enhancement          = true
      debugging extensions                   = true
      page size extensions                   = true
      time stamp counter                     = true
      RDMSR and WRMSR support                = true
      physical address extensions            = true
      machine check exception                = true
      CMPXCHG8B inst.                        = true
      APIC on chip                           = true
      SYSENTER and SYSEXIT                   = true
      memory type range registers            = true
      PTE global bit                         = true
      machine check architecture             = true
      conditional move/compare instruction   = true
      page attribute table                   = true
:
```

◦ **What happens if you disable the functionality and restart the test VM?**
Nothing happens in this case, it shows GenuineIntel


Activities
Terminal
Sun 17:58
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996: ~
File Edit View Search Terminal Help
Ubuntu Software

```
inside-virt@insidevirt-Standard-PC-i440FX-PIIX-1996:~$ dmesg
[    0.000000] random: get_random_bytes called from start_kernel+0x42/0x4e1 with crng_init=0
[    0.000000] Linux version 4.13.0-16-generic (buildd@lcy01-02) (gcc version 7.2.0 (Ubuntu 7.2.0-8ubunt
u2)) #19-Ubuntu SMP Wed Oct 11 18:35:14 UTC 2017 (Ubuntu 4.13.0-16.19-generic 4.13.4)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-4.13.0-16-generic root=UUID=3c005dc1-b5c0-4439-961
5-3e9036ef9dce ro quiet splash vt.handoff=7
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[                 Centaur CentaurHauls
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000003ffdffff] usable
[    0.000000] BIOS-e820: [mem 0x000000003ffe0000-0x000000003fffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] random: fast init done
[    0.000000] SMBIOS 2.8 present.
[    0.000000] DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.10.1-1ubuntu1 04/01/2014
```