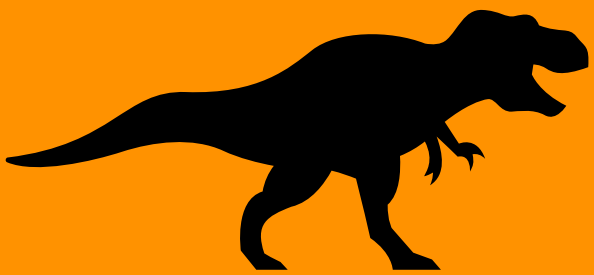
## KERNEL MODULE PROGRAMMING

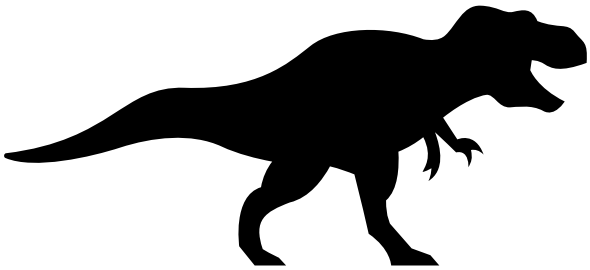
# OPERATING SYSTEM




COLLABORATORS NAME & ID :
MARYAM ALIKARAMI 9731045
MAHAN AHMADVAND 9731071

KERNEL MODULE PROGRAMMING

# OPERATING SYSTEM



COLLABORATORS NAME & ID :
MARYAM ALIKARAMI 9731045
MAHAN AHMADVAND 9731071

# OPERATING SYSTEM LABORATORY

## KERNEL MODULE PROGRAMMING


INSTRUCTOR :

ARMAN GHEISARI

COLLABORATORS :

MARYAM ALIKARAMI

MAHAN AHMADVAND

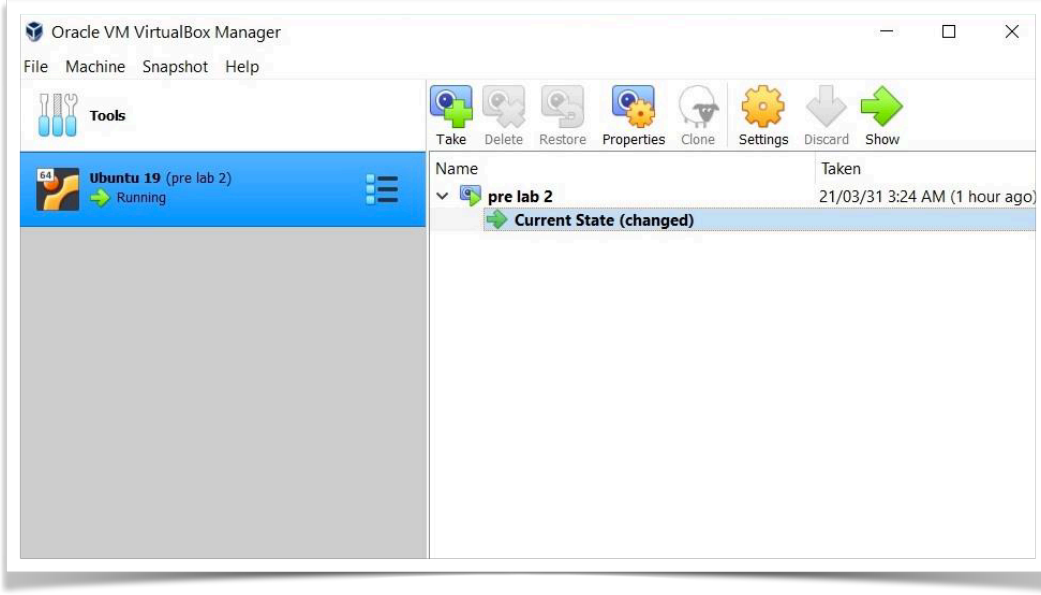
# QUESTION 1

در این بخش از آزمایش قصد داریم تا یک ماژول هسته را بارگذاری و حذف کنیم و با بررسی بافر سابقه ی هسته مطمئن شویم که این فرآیند را به درستی طی کرده ایم.

در ابتدا بهتر است اشاره کنیم که ماژول های هسته چه هستند. Kernel Modules یا ماژول های هسته عبارتند از تکه کدهایی که در هنگام run-time می توانند در کرنل بارگذاری یا از آن حذف شوند و برای اجرای آن ها نیازی نیست که سیستم مجددا راه اندازی شود.

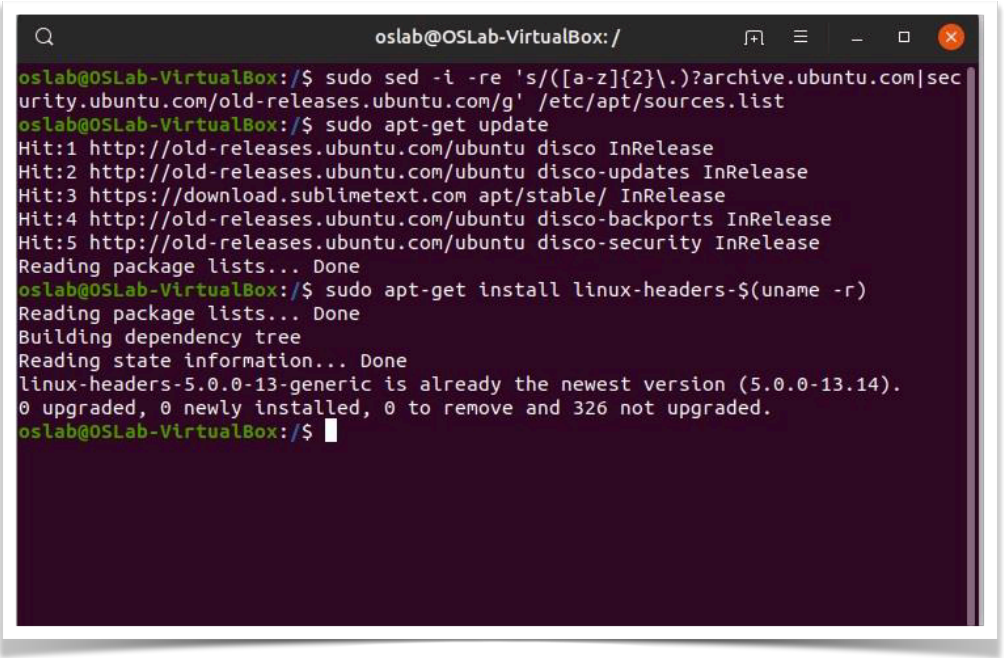
حال به انجام این بخش از آزمایش می پردازیم.

از آن جایی که ماژول های هسته به صورت مستقیم با کرنل در ارتباط هستند و هرگونه خطا و اشکال در آن ها می تواند باعث بروز اشکال در کل سیستم گردد، قبل از شروع کار از وضعیت فعلی ماشین مجازی خود snapshot می گیریم تا در صورت نیاز بتوانیم به شرایطی که قبل از شروع آزمایش داشتیم بازگردیم.




در مرحله ی بعدی برای اطمینان از اینکه هدرهای موردنیاز ما نصب شده و آپدیت هستند، مراحل زیر را طی می کنیم :

ابتدا دستور sudo sed -i -re 's/([a-z]{2}\.)?archive.ubuntu.com|security.ubuntu.com/old-releases.ubuntu.com/g' /etc/apt/sources.list و سپس به ترتیب دستورات sudo apt -get update و sudo apt-get install linux-headers-$(uname -r) را در ترمینال وارد می کنیم.

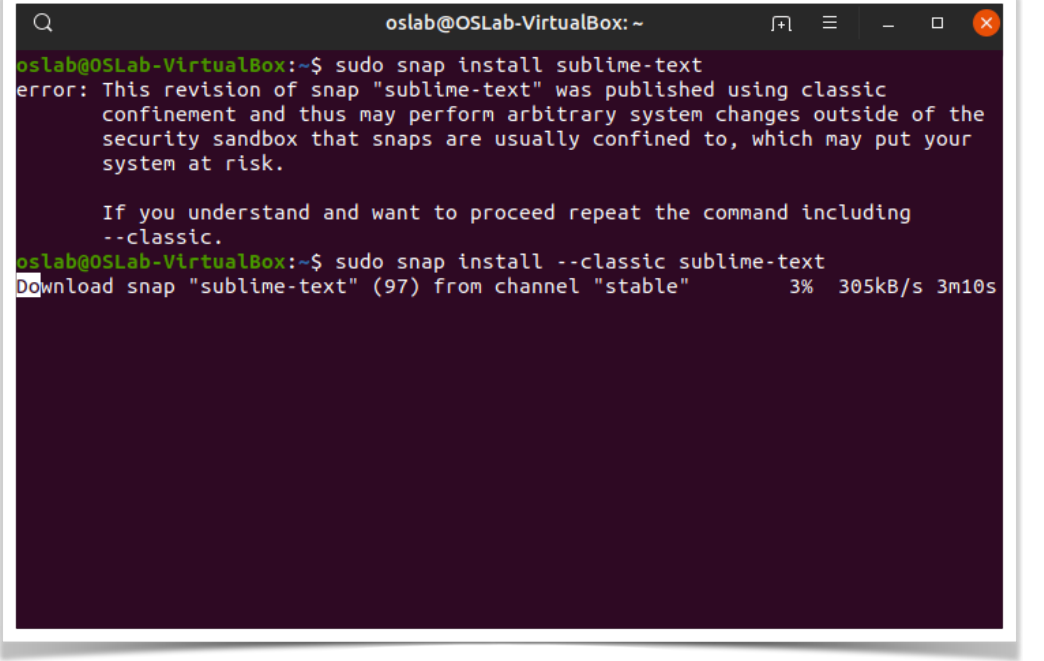



دستور sed یا stream editor دستوری است که این قابلیت را به کاربر می دهد تا بدون بازکردن یک فایل در ادیتور و فقط با اجرای این دستور، فایل را ادیت کند و فرآیندهایی همچون insert، deletion، replacement، find و search را به روی آن فایل اجرا کند.

از دستور apt-get برای مدیریت پکیج ها به واسطه ی کار با بخش APT(Advanced Packaging Tool) در لینوکس، استفاده می شود.

از این دستور برای حذف، نصب و به روزرسانی پکیج ها و نرم افزارها استفاده می شود.

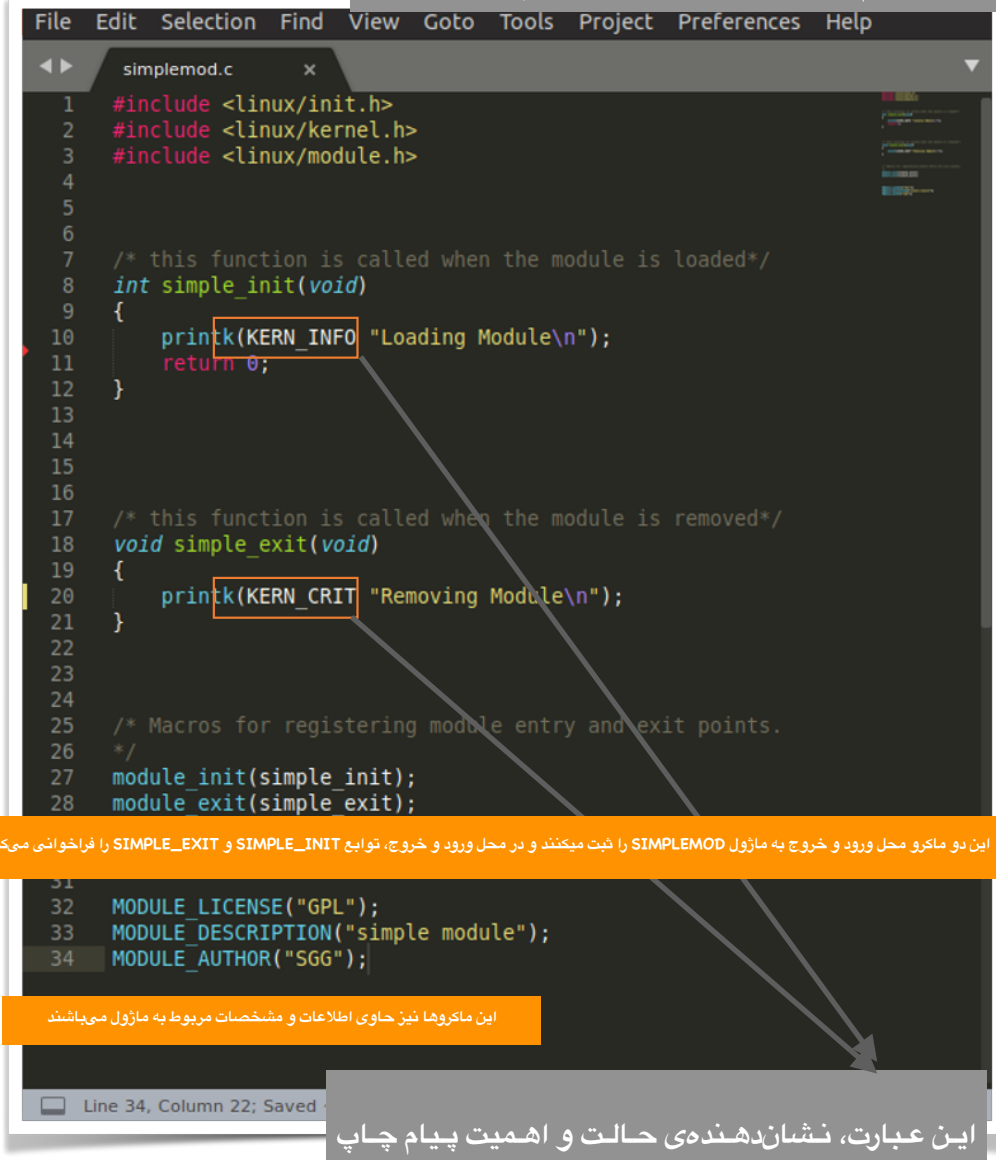
بعد از اینکه مطمئن شدیم هدرهای موردنظر ما نصب هستند، ادیتور sublime-text را با استفاده از دستور sudo snap install sublime-text نصب می کنیم تا بتوانیم ادیت فایلهای خود را در محیطی کارآمدتر انجام دهیم.




snapp یک سیستم مدیریت پکیج در لینوکس است که به واسطه ی آن می توان به راحتی بسیاری از برنامه هایی را که در این سیستم پکیج شده اند را دانلود و نصب کرد. این سیستم از Ubuntu 16.04 LTS به بعد روی تمام ورژن های اوبونتو نصب است و تمام برنامه هایی که با استفاده از snapp نصب شوند به صورت اتوماتیک آپدیت خواهند شد.

پس از نصب، sublime-text را باز می کنیم تا کد مربوط به ماژول خود را در آن وارد و ادیت کنیم. (از آنجایی که کد این ماژول را آماده داریم آن را کپی می کنیم و در فرمت یک فایل c. ذخیره می کنیم).

دستور PRINTK معادل دستور PRINTF است با این تفاوت که پیام خود را در بافر سابقه هسته چاپ می‌کند.




این دو ماکرو محل ورود و خروج به ماژول SIMPLEMOD را ثبت میکنند و در محل ورود و خروج، توابع SIMPLE_INIT و SIMPLE_EXIT را فراخوانی می‌کنند.

این ماکروها نیز حاوی اطلاعات و مشخصات مربوط به ماژول می‌باشند

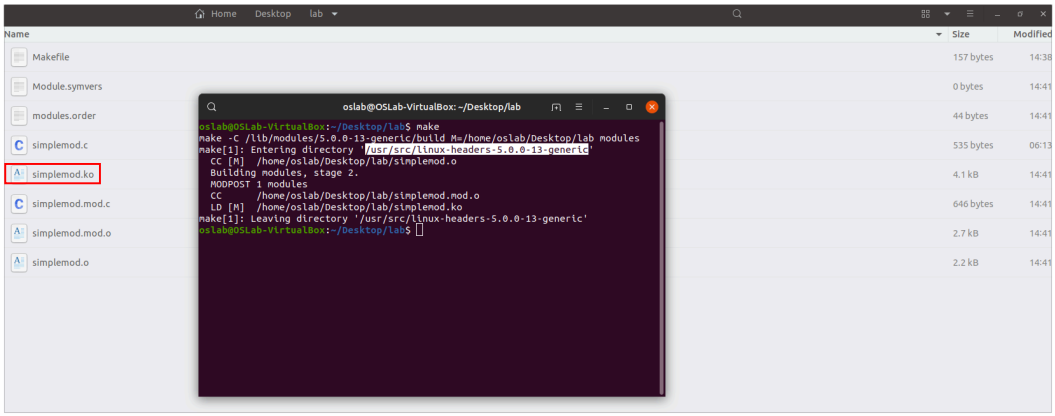
این عبارت، نشان‌دهنده‌ی حالت و اهمیت پیام چاپ شده است. طبق جدول اولویت‌ها kern_info نشان دهنده‌ی یک پیام عادی است اما kern_crit یک پیام critical است که اولویت بالاتری دارد و در صورت مشاهده باید فورا به آن رسیدگی شود. در اینجا این عبارت را تغییر دادیم تا ماژول ما چند حالت متفاوت را در بگیرد. به همین دلیل است که پیام removing module به رنگ قرمز چاپ خواهد شد.

فایل بدون پسوند دیگری شامل قوانین مربوط به کامپایل simplemod.c را در هیمن دایرکتوری ایجاد می کنیم و نام آن را Makefile می گذاریم.(به همین دلیل تغییر دادن نام ماژول نیاز است تا در کد آماده ای که برای makefile در اختیار داریم نیز تغییر ایجاد کنیم)

هرگاه که می خواهیم از دستور make استفاده کنیم به یک makefile نیز نیاز است که ارتباط فایلهای درون برنامه ی ما را توضیح می دهد.


حالا در همین دایرکتوری فعلی (Desktop/lab) که فایل های ما درون آن قرار دارند، ترمینال را باز می کنیم و دستور make را وارد می کنیم. از این دستور برای کامپایل کردن ماژول ها و پروژه های بزرگ استفاده می شود. پس از کامپایل، فایل simplemod.ko در همین دایرکتوری ایجاد می شود. پسوند ko. برای ماژول های هسته در نظر گرفته می شود.

در همین مرحله، آدرس entering directory را در جایی سیو می کنیم چون برای مراحل بعدی به آن نیاز داریم.




حالا که ماژول هسته ی ما ساخته شده، می توانیم آن را به کرنل اضافه و از آن حذف کنیم. برای اینکه به این فرآیند نظارت داشته باشیم، تب جدیدی در ترمینال باز می کنیم و دستور tail -f/var/log/syslog را وارد می کنیم تا لاگ های سیستم را زیر نظر بگیریم و ببینیم که آیا خروجی دلخواه خود را می گیریم یا خیر (برای همین منظور می توان از دستور dmseg استفاده کرد که محتویات بافر سابقه هسته را چاپ می کند) طبق کد simplemod.c، انتظار داریم که با لود کردن ماژول پیام Loading Module و با حذف آن پیام Removing Module چاپ شوند.

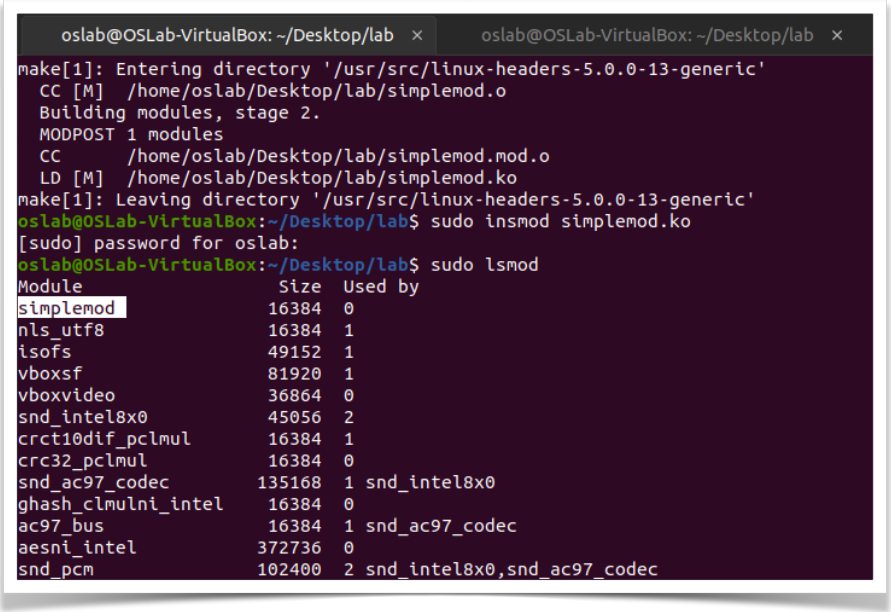
حالا با استفاده از دستور sudo insmod simple mod.ko این ماژول را در کرنل لود می کنیم.

```
oslab@OSLab-VirtualBox:~/Desktop/lab$ make
make -C /lib/modules/5.0.0-13-generic/build M=/home/oslab/Desktop/lab modules
make[1]: Entering directory '/usr/src/linux-headers-5.0.0-13-generic'
  CC [M]  /home/oslab/Desktop/lab/simplemod.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/oslab/Desktop/lab/simplemod.mod.o
  LD [M]  /home/oslab/Desktop/lab/simplemod.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.0.0-13-generic'
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo insmod simplemod.ko
[sudo] password for oslab:
oslab@OSLab-VirtualBox:~/Desktop/lab$
```

حالا اگر به تب دوم که دستور tail را در آن اجرا کرده بودیم نگاه کنیم، می بینیم که عبارت "loading module" طبق انتظار ما چاپ شده است.

```
oslab@OSLab-VirtualBox: ~/Desktop/lab ×   oslab@OSLab-VirtualBox: ~/Desktop/lab ×
Mar 31 15:18:01 OSLab-VirtualBox dbus-daemon[665]: [system] Activating via syste
md: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname
1.service' requested by ':1.868' (uid=1000 pid=29288 comm="rhythmbox " label="un
confined")
Mar 31 15:18:01 OSLab-VirtualBox systemd[1]: Starting Hostname Service...
Mar 31 15:18:02 OSLab-VirtualBox dbus-daemon[665]: [system] Successfully activat
ed service 'org.freedesktop.hostname1'
Mar 31 15:18:02 OSLab-VirtualBox systemd[1]: Started Hostname Service.
Mar 31 15:18:05 OSLab-VirtualBox rhythmbox[29288]: Can't set a parent on widget
which has a parent
Mar 31 15:18:32 OSLab-VirtualBox systemd[1]: systemd-hostnamed.service: Succeede
d.
Mar 31 15:21:30 OSLab-VirtualBox kernel: [49460.876060] Loading Module
Mar 31 15:21:48 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Activating via systemd: service name='org.freedesktop.Tracker1.Miner.Extract' un
it='tracker-extract.service' requested by ':1.53' (uid=1000 pid=2074 comm="/usr/
lib/tracker/tracker-miner-fs " label="unconfined")
Mar 31 15:21:48 OSLab-VirtualBox systemd[1601]: Starting Tracker metadata extrac
tor...
Mar 31 15:21:49 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 31 15:21:49 OSLab-VirtualBox systemd[1601]: Started Tracker metadata extract
or.
```

در این حالت اگر دستور sudo lsmod را وارد کنیم که ماژول های فعلی هسته را لیست می کند، می توانیم ماژول خود را میان آن ها ببینیم.




با دستور sudo lsmod | grep [module name] می توانیم به دنبال یک ماژول خاص که در حال حاضر در هسته لود شده است بگردیم، اگر این دستور را برای simplemod اجرا کنیم، آن را می یابیم.

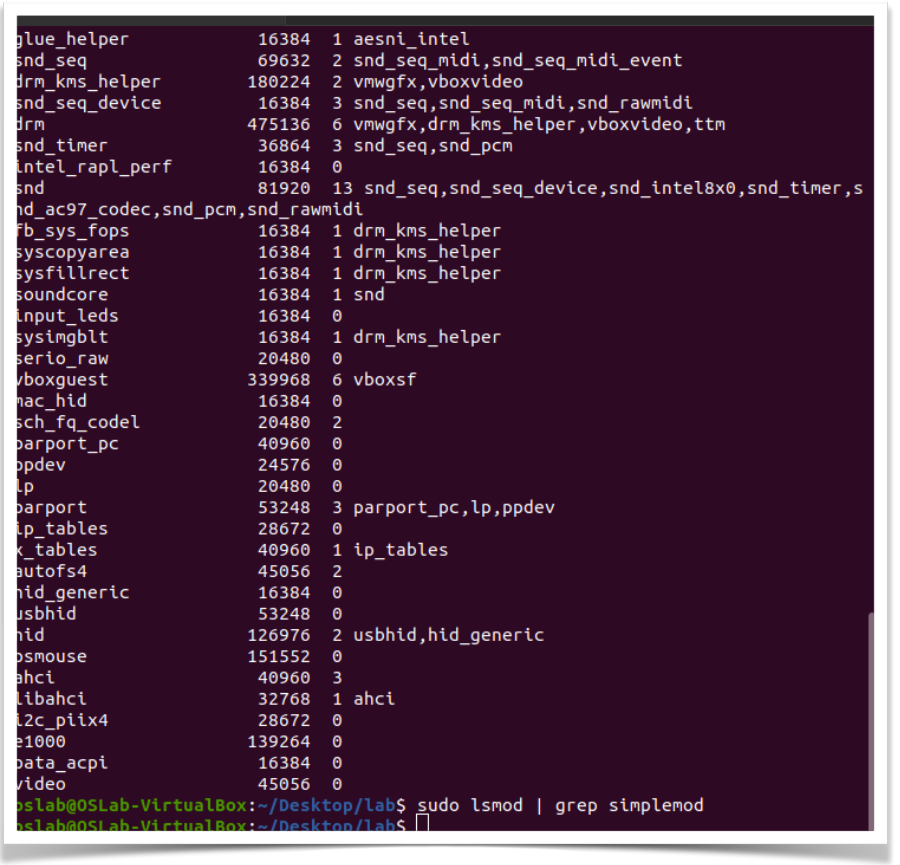
در این مرحله قصد داریم ماژولی که بارگذاری کردیم را از کرنل حذف کنیم. برای این کار از دستور sudo rmmod [module name] استفاده می کنیم.

```
pata_acpi              16384  0
video                  45056  0
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo lsmod | grep simplemod
simplemod              16384  0
oslab@OSLab-VirtualBox:~/Desktop/lab$ sudo rmmod simplemod
oslab@OSLab-VirtualBox:~/Desktop/lab$
```

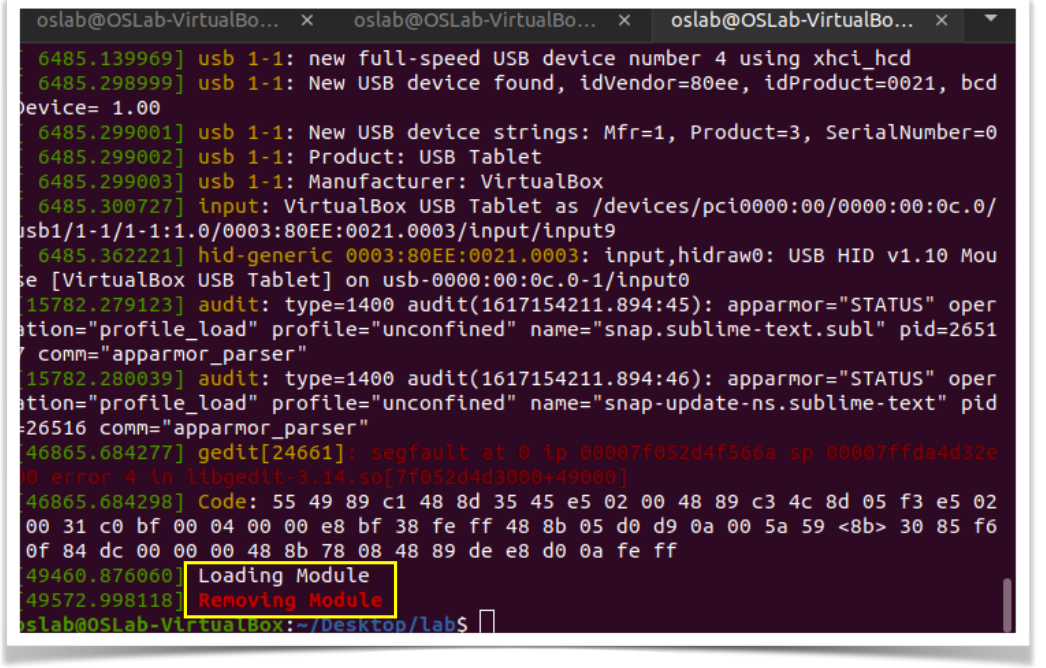
پس از اجرای این دستور در تب دوم می بینیم که عبارت removing module چاپ شده است.

```
oslab@OSLab-VirtualBox: ~/Desktop/lab ×   oslab@OSLab-VirtualBox: ~/Desktop/lab ×
it='tracker-extract.service' requested by ':1.53' (uid=1000 pid=2074 comm="/usr/
lib/tracker/tracker-miner-fs " label="unconfined")
Mar 31 15:23:06 OSLab-VirtualBox systemd[1601]: Starting Tracker metadata extrac
tor...
Mar 31 15:23:06 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 31 15:23:06 OSLab-VirtualBox systemd[1601]: Started Tracker metadata extract
or.
Mar 31 15:23:16 OSLab-VirtualBox systemd[1601]: tracker-extract.service: Succeed
ed.
Mar 31 15:23:22 OSLab-VirtualBox kernel: [49572.998118] Removing Module
Mar 31 15:23:25 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Activating via systemd: service name='org.freedesktop.Tracker1.Miner.Extract' un
it='tracker-extract.service' requested by ':1.53' (uid=1000 pid=2074 comm="/usr/
lib/tracker/tracker-miner-fs " label="unconfined")
Mar 31 15:23:25 OSLab-VirtualBox systemd[1601]: Starting Tracker metadata extrac
tor...
Mar 31 15:23:25 OSLab-VirtualBox dbus-daemon[1630]: [session uid=1000 pid=1630]
Successfully activated service 'org.freedesktop.Tracker1.Miner.Extract'
Mar 31 15:23:25 OSLab-VirtualBox systemd[1601]: Started Tracker metadata extract
or.
Mar 31 15:23:35 OSLab-VirtualBox systemd[1601]: tracker-extract.service: Succeed
ed.
```

بعد از حذف کردن simplemod اگر از ماژول های هسته لیست بگیریم یا مجددا به دنبال simplemod بگردیم، آن را نخواهیم یافت.




همانطور که گفتیم با دستور dmesg نیز می توانیم پیام های بافر سابقه ی هسته را رویت کنیم. دلیل قرمز بودن عبارت remove را در بخش توضیحات کد شرح دادیم.


oslab@OSLab-VirtualBo...
oslab@OSLab-VirtualBo...
oslab@OSLab-VirtualBo...
6485.139969] usb 1-1: new full-speed USB device number 4 using xhci_hcd
6485.298999] usb 1-1: New USB device found, idVendor=80ee, idProduct=0021, bcd
Device= 1.00
6485.299001] usb 1-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
6485.299002] usb 1-1: Product: USB Tablet
6485.299003] usb 1-1: Manufacturer: VirtualBox
6485.300727] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:0c.0/
usb1/1-1/1-1:1.0/0003:80EE:0021.0003/input/input9
6485.362221] hid-generic 0003:80EE:0021.0003: input,hidraw0: USB HID v1.10 Mou
se [VirtualBox USB Tablet] on usb-0000:00:0c.0-1/input0
15782.279123] audit: type=1400 audit(1617154211.894:45): apparmor="STATUS" oper
ation="profile_load" profile="unconfined" name="snap.sublime-text.subl" pid=2651
7 comm="apparmor_parser"
15782.280039] audit: type=1400 audit(1617154211.894:46): apparmor="STATUS" oper
ation="profile_load" profile="unconfined" name="snap-update-ns.sublime-text" pid
=26516 comm="apparmor_parser"
46865.684277] gedit[24661]: segfault at 0 ip 00007f052d4f566a sp 00007ffda4d32e
00 error 4 in libgedit-3.14.so[7f052d4d3000+49000]
46865.684298] Code: 55 49 89 c1 48 8d 35 45 e5 02 00 48 89 c3 4c 8d 05 f3 e5 02
00 31 c0 bf 00 04 00 00 e8 bf 38 fe ff 48 8b 05 d0 d9 0a 00 5a 59 <8b> 30 85 f6
0f 84 dc 00 00 00 48 8b 78 08 48 89 de e8 d0 0a fe ff
49460.876060] Loading Module
49572.998118] Removing Module
oslab@OSLab-VirtualBox:~/Desktop/lab$

# QUESTION 2

# THE END