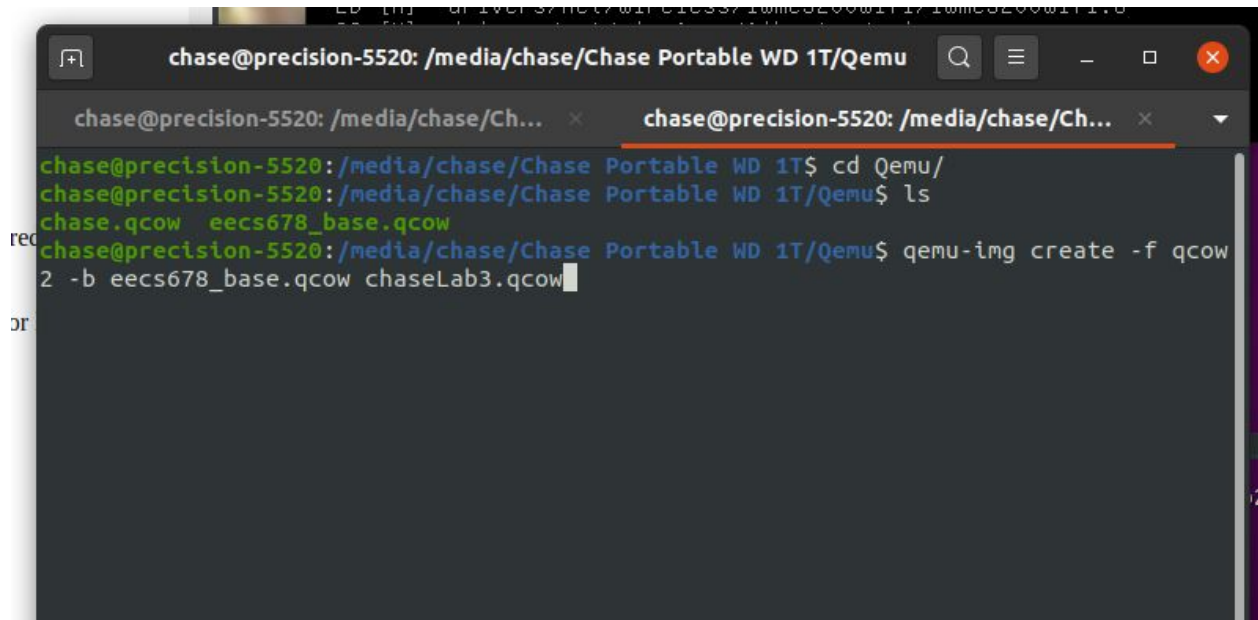


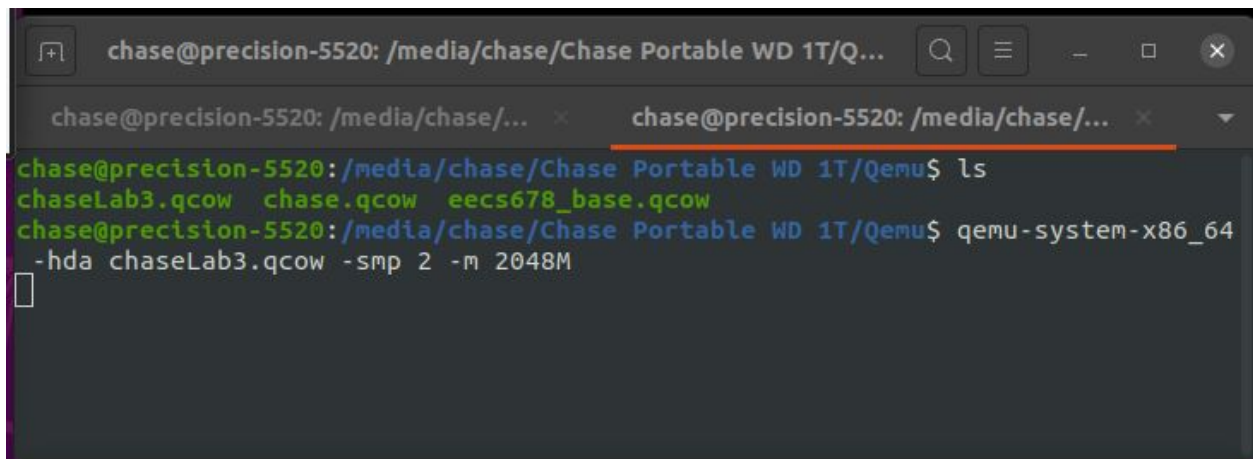
Lab 3



A terminal window titled "chase@precision-5520: /media/chase/Chase Portable WD 1T/Qemu" with two tabs. The active tab shows the following commands and output:

```
chase@precision-5520:/media/chase/Chase Portable WD 1T$ cd Qemu/  
chase@precision-5520:/media/chase/Chase Portable WD 1T/Qemu$ ls  
chase.qcow  eeecs678_base.qcow  
chase@precision-5520:/media/chase/Chase Portable WD 1T/Qemu$ qemu-img create -f qcow  
2 -b eeecs678_base.qcow chaseLab3.qcow
```

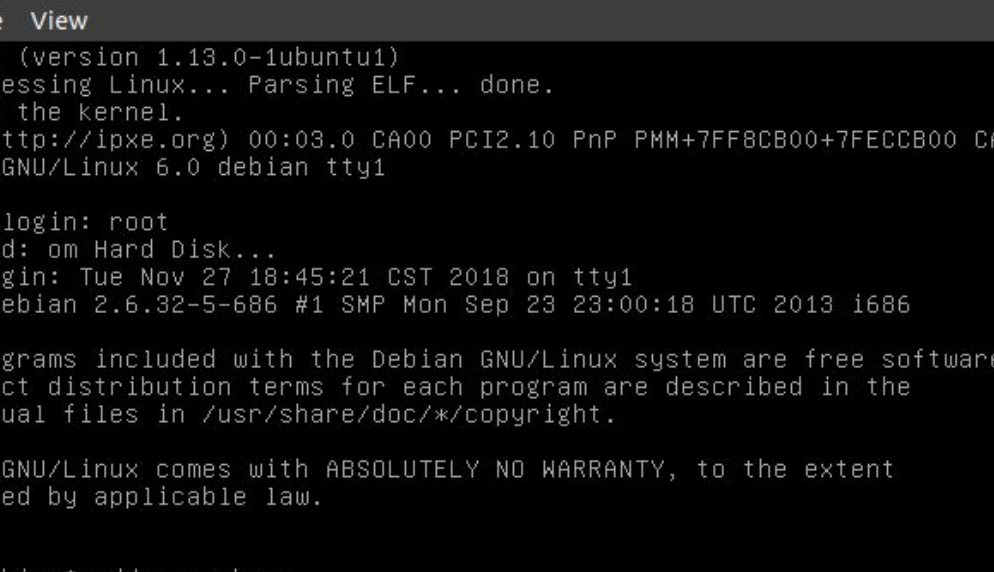
- 1.) Created differential image of file copied from cycle servers in lab2 and named it chaseLab3.qcow



A terminal window titled "chase@precision-5520: /media/chase/Chase Portable WD 1T/Q..." with two tabs. The active tab shows the following commands and output:

```
chase@precision-5520:/media/chase/Chase Portable WD 1T/Qemu$ ls  
chaseLab3.qcow  chase.qcow  eeecs678_base.qcow  
chase@precision-5520:/media/chase/Chase Portable WD 1T/Qemu$ qemu-system-x86_64  
-hda chaseLab3.qcow -smp 2 -m 2048M
```

- 2.) Booted system with 2 cores and 2048M RAM



```
Machine  View
SeaBIOS (version 1.13.0-1ubuntu1)
Decompressing Linux... Parsing ELF... done.
Booting the kernel.
iPXE (http://ipxe.org) 00:03.0 CA00 PCI2.10 PnP PMM+7FF8CB00+7FECCB00 CA00
Debian GNU/Linux 6.0 debian tty1

debian login: root
Password: om Hard Disk...
Last login: Tue Nov 27 18:45:21 CST 2018 on tty1
Linux debian 2.6.32-5-686 #1 SMP Mon Sep 23 23:00:18 UTC 2013 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

[~]
root@debian$ adduser chase
```

3.) Added user

[illegible]

4.) Added user to /etc/sudoers

```
[~]  
root@debian$ usermod -a -G sudo chase  
  
[~]  
root@debian$ mkdir /home/chase/kernel  
  
[~]  
root@debian$ mv ~/linux-2.6.32.60/ /home/chase/kernel/  
  
[~]  
root@debian$ chown -R chase:chase /home/chase/kernel/  
  
[~]  
root@debian$ apt-get install sudo_
```

- 5.) Added myself to sudo group, made a folder called kernel, changed ownership to myself, install sudo.

```
[~]  
root@debian$ cp /root/.vimrc /home/chase  
  
[~]  
root@debian$ chown chase:chase /home/chase/.vimrc  
  
[~]  
root@debian$ su chase  
chase@debian:/root$ sudo apt-get install libz-dev_
```

- 6.) Copied .vimrc from /root into my home folder and changed ownership, then downloaded libz-dev

```
QEMU
Machine View
#3) With great power comes great responsibility.

[sudo] password for chase:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'zlib1g-dev' instead of 'libz-dev'
The following NEW packages will be installed:
  zlib1g-dev
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 186 kB of archives.
After this operation, 418 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  zlib1g-dev
Install these packages without verification [y/N]? y
Get:1 http://archive.debian.org/debian/ squeeze/main zlib1g-dev i386 1:1.2.3.4.dfsg-3 [186 kB]
Fetched 186 kB in 6s (28.1 kB/s)
Selecting previously deselected package zlib1g-dev.
(Reading database ... 23875 files and directories currently installed.)
Unpacking zlib1g-dev (from .../zlib1g-dev_1%3a1.2.3.4.dfsg-3_i386.deb) ...
Processing triggers for man-db ...
Setting up zlib1g-dev (1:1.2.3.4.dfsg-3) ...
chase@debian:/root$ cd
chase@debian:~$ cd /home/chase/kernel/linux-2.6.32.60/_
```

7.) Changed into linux-2.6.32.60 directory

```
Machine View
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'zlib1g-dev' instead of 'libz-dev'
The following NEW packages will be installed:
  zlib1g-dev
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 186 kB of archives.
After this operation, 418 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  zlib1g-dev
Install these packages without verification [y/N]? y
Get:1 http://archive.debian.org/debian/ squeeze/main zlib1g-dev i386 1:1.2.3.4.dfsg-3 [186 kB]
Fetched 186 kB in 6s (28.1 kB/s)
Selecting previously deselected package zlib1g-dev.
(Reading database ... 23875 files and directories currently installed.)
Unpacking zlib1g-dev (from .../zlib1g-dev_1%3a1.2.3.4.dfsg-3_i386.deb) ...
Processing triggers for man-db ...
Setting up zlib1g-dev (1:1.2.3.4.dfsg-3) ...
chase@debian:/root$ cd
chase@debian:~$ cd /home/chase/kernel/linux-2.6.32.60/
chase@debian:~/kernel/linux-2.6.32.60$ mkdir hello
chase@debian:~/kernel/linux-2.6.32.60$ cd hello
chase@debian:~/kernel/linux-2.6.32.60/hello$ vi hello.c_
```

8.) Made directory "hello", changed locations into it and opened up hello.c

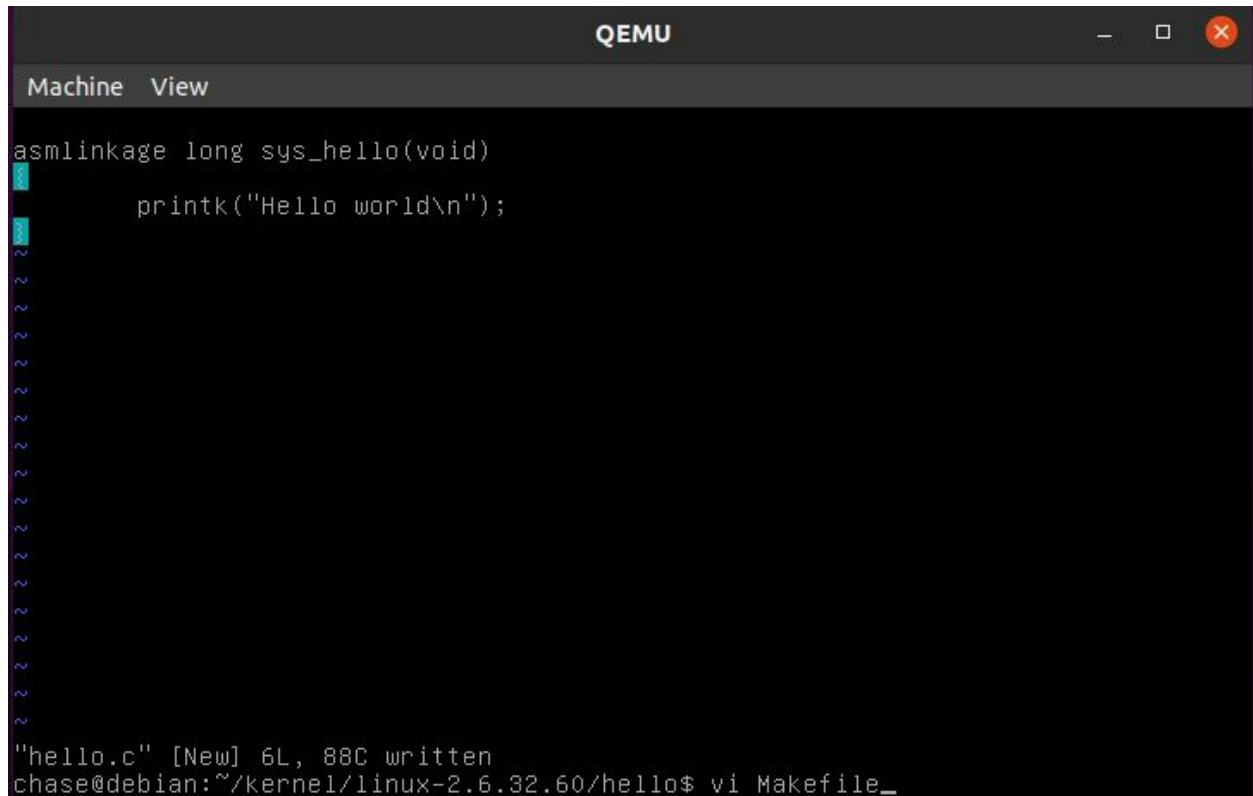
A screenshot of a QEMU window titled "QEMU" with standard window controls. The main area is a dark-themed text editor showing a C program. The code includes a header, a function definition, and a call to printk. The editor has a line number column on the left and a status bar at the bottom.

```
Machine View
#include<linux/kernel.h>

asm linkage long sys_hello(void)
1     printk("Hello world\n");
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
-- INSERT --
```

6,2 All

9.) Created hello.c program



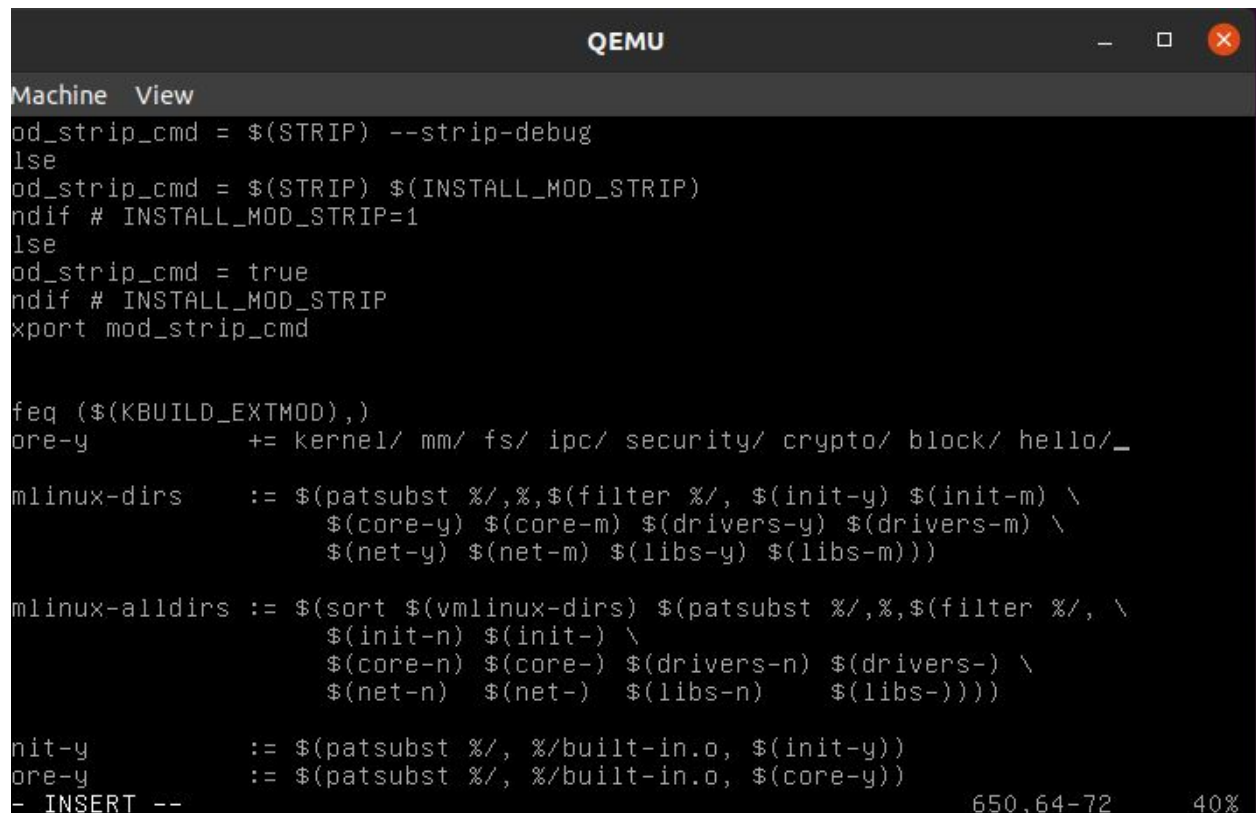
The screenshot shows a QEMU terminal window with a dark background. The title bar at the top says "QEMU" and has standard window controls. Below the title bar is a menu bar with "Machine" and "View". The terminal displays the assembly of a C file named "hello.c". The assembly code is shown in a light blue font on a dark background. The code starts with "asmlinkage long sys_hello(void)" and "printk(\"Hello world\\n\");". There are several lines of assembly code below, including "movl \$0, %eax", "movl \$0, %ecx", "movl \$0, %edx", "movl \$0, %ebx", "movl \$0, %esi", "movl \$0, %edi", "movl \$0, %ebp", "movl \$0, %esp", "movl \$0, %eip", "movl \$0, %ebp", "movl \$0, %esp", "movl \$0, %eip". The terminal also shows the command "chase@debian:~/kernel/linux-2.6.32.60/hello\$ vi Makefile_" and the output "hello.c" [New] 6L, 88C written.

```
Machine View
asmlinkage long sys_hello(void)
    printk("Hello world\\n");
    movl $0, %eax
    movl $0, %ecx
    movl $0, %edx
    movl $0, %ebx
    movl $0, %esi
    movl $0, %edi
    movl $0, %ebp
    movl $0, %esp
    movl $0, %eip
    movl $0, %ebp
    movl $0, %esp
    movl $0, %eip
"hello.c" [New] 6L, 88C written
chase@debian:~/kernel/linux-2.6.32.60/hello$ vi Makefile_
```

10.) Opened Makefile

[illegible]

- 11.) Changed makefile to contain necessary statement.

A screenshot of a QEMU window titled "QEMU" with standard window controls. The window displays a Makefile snippet in a dark-themed editor. The text is as follows:

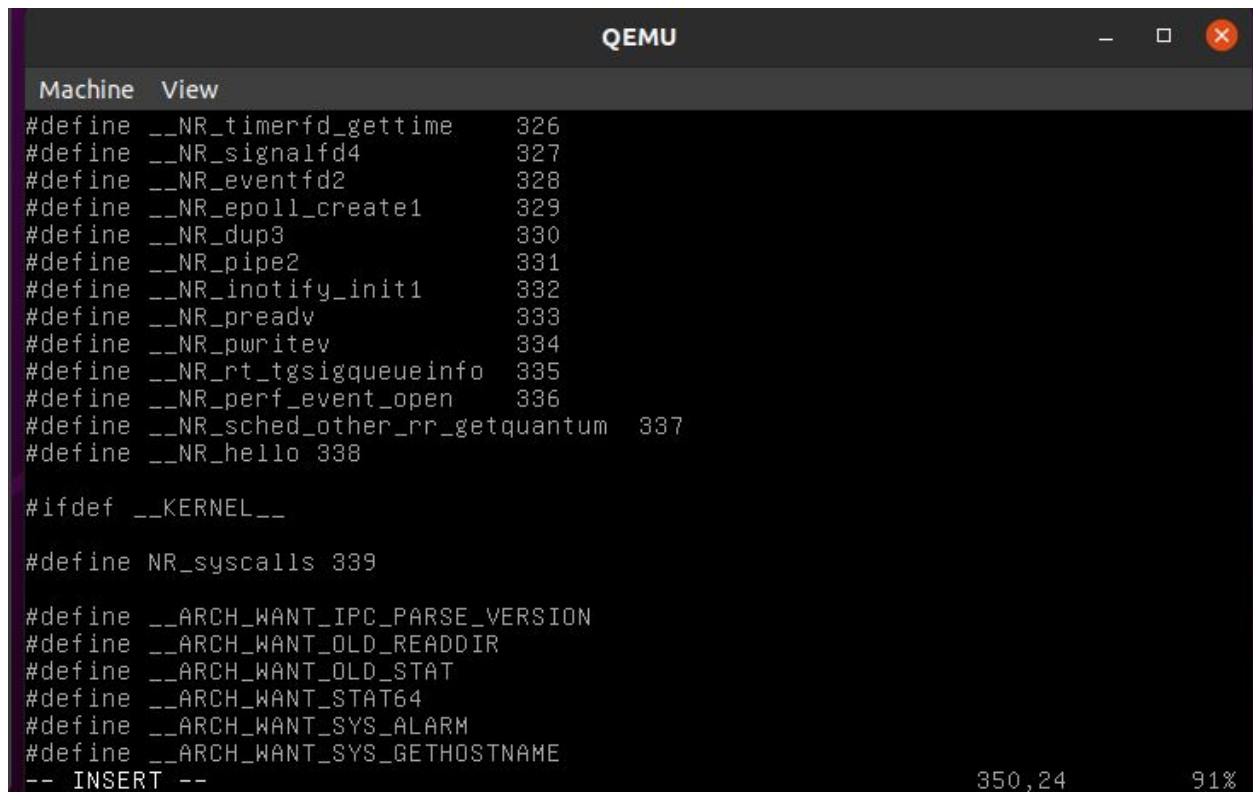
```
Machine View
od_strip_cmd = $(STRIP) --strip-debug
else
od_strip_cmd = $(STRIP) $(INSTALL_MOD_STRIP)
endif # INSTALL_MOD_STRIP=1
else
od_strip_cmd = true
endif # INSTALL_MOD_STRIP
export mod_strip_cmd

ifeq ($(KBUILD_EXTMOD),)
core-y      += kernel/ mm/ fs/ ipc/ security/ crypto/ block/ hello/_
vmlinux-dirs := $(patsubst %/,%, $(filter %/, $(init-y) $(init-m) \
$(core-y) $(core-m) $(drivers-y) $(drivers-m) \
$(net-y) $(net-m) $(libs-y) $(libs-m)))
vmlinux-alldirs := $(sort $(vmlinux-dirs) $(patsubst %/,%, $(filter %/, \
$(init-n) $(init-) \
$(core-n) $(core-) $(drivers-n) $(drivers-) \
$(net-n) $(net-) $(libs-n) $(libs-))))
init-y      := $(patsubst %/, %/built-in.o, $(init-y))
core-y      := $(patsubst %/, %/built-in.o, $(core-y))
- INSERT --                                     650,64-72      40%
```

12.) Added "hello/" to the existing makefile


```
QEMU
Machine  View
.long sys_tee /* 315 */
.long sys_vmsplice
.long sys_move_pages
.long sys_getcpu
.long sys_epoll_pwait
.long sys_utimensat /* 320 */
.long sys_signalfd
.long sys_timerfd_create
.long sys_eventfd
.long sys_fallocate
.long sys_timerfd_settime /* 325 */
.long sys_timerfd_gettime
.long sys_signalfd4
.long sys_eventfd2
.long sys_epoll_create1
.long sys_dup3 /* 330 */
.long sys_pipe2
.long sys_inotify_init1
.long sys_preadv
.long sys_pwritev
.long sys_rt_tgsigqueueinfo /* 335 */
.long sys_perf_event_open
.long sys_sched_other_rr_getquantum
.long sys_hello
- INSERT -- 340,17-24 Bot
```

13.) Edited syscall_table_32.S by adding .long sys_hello

A screenshot of a QEMU terminal window. The window has a title bar with the text "QEMU" and standard window controls (minimize, maximize, close). Below the title bar is a menu bar with "Machine" and "View". The main area of the window displays a list of kernel constants and their values, followed by a conditional compilation block for the kernel. The constants are: __NR_timerfd_gettime (326), __NR_signalfd4 (327), __NR_eventfd2 (328), __NR_epoll_create1 (329), __NR_dup3 (330), __NR_pipe2 (331), __NR_inotify_init1 (332), __NR_preadv (333), __NR_pwritev (334), __NR_rt_tsigqueueinfo (335), __NR_perf_event_open (336), __NR_sched_other_rr_getquantum (337), and __NR_hello (338). The conditional block starts with #ifdef __KERNEL__ and defines NR_syscalls as 339. It then lists several __ARCH_WANT_* macros: __ARCH_WANT_IPC_PARSE_VERSION, __ARCH_WANT_OLD_READDIR, __ARCH_WANT_OLD_STAT, __ARCH_WANT_STAT64, __ARCH_WANT_SYS_ALARM, and __ARCH_WANT_SYS_GETHOSTNAME. The block ends with -- INSERT --. The bottom right corner of the terminal shows the coordinates 350,24 and the zoom level 91%.

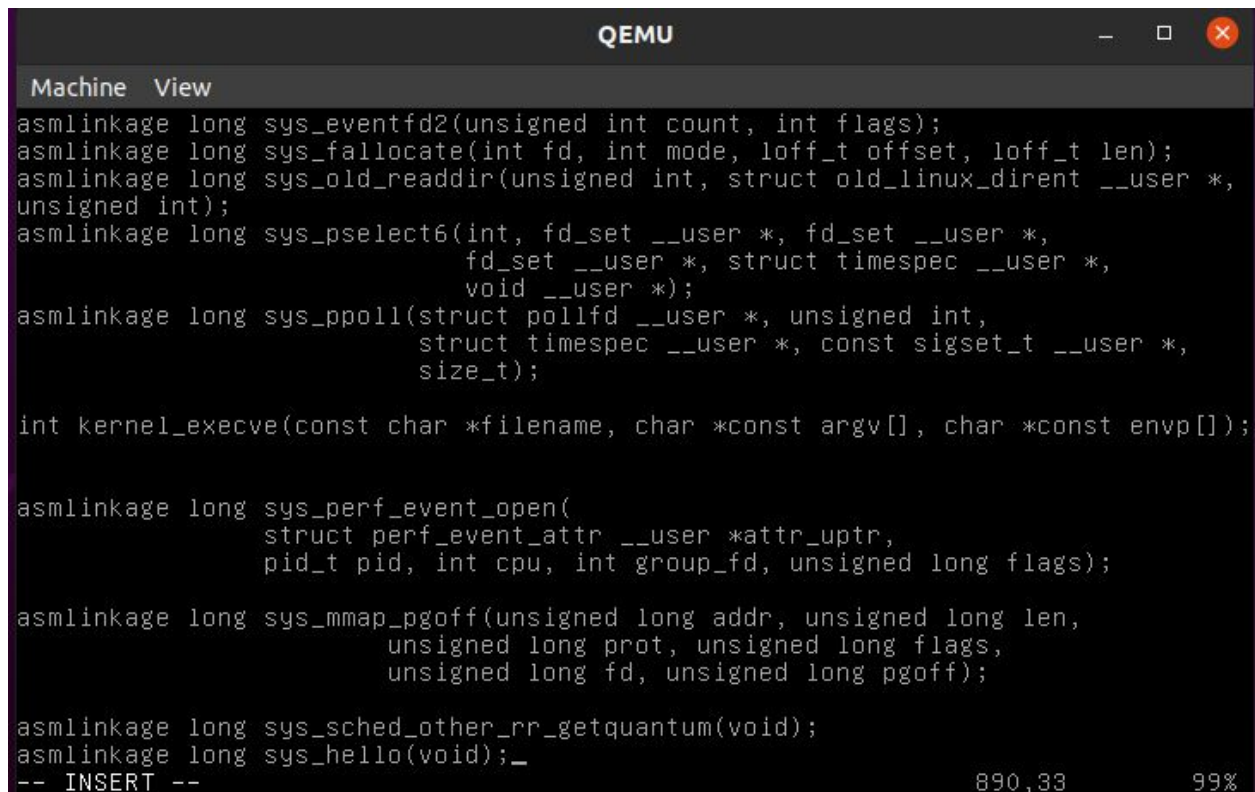
```
Machine View
#define __NR_timerfd_gettime 326
#define __NR_signalfd4 327
#define __NR_eventfd2 328
#define __NR_epoll_create1 329
#define __NR_dup3 330
#define __NR_pipe2 331
#define __NR_inotify_init1 332
#define __NR_preadv 333
#define __NR_pwritev 334
#define __NR_rt_tsigqueueinfo 335
#define __NR_perf_event_open 336
#define __NR_sched_other_rr_getquantum 337
#define __NR_hello 338

#ifdef __KERNEL__

#define NR_syscalls 339

#define __ARCH_WANT_IPC_PARSE_VERSION
#define __ARCH_WANT_OLD_READDIR
#define __ARCH_WANT_OLD_STAT
#define __ARCH_WANT_STAT64
#define __ARCH_WANT_SYS_ALARM
#define __ARCH_WANT_SYS_GETHOSTNAME
-- INSERT --
350,24 91%
```

- 14.) Modified the file unistd_32.h to add a definition of hello, then modified the syscalls definition to handle the new line.



```
Machine View
asmlinkage long sys_eventfd2(unsigned int count, int flags);
asmlinkage long sys_fallocate(int fd, int mode, loff_t offset, loff_t len);
asmlinkage long sys_old_readdir(unsigned int, struct old_linux_dirent __user *,
unsigned int);
asmlinkage long sys_pselect6(int, fd_set __user *, fd_set __user *,
fd_set __user *, struct timespec __user *,
void __user *);
asmlinkage long sys_ppoll(struct pollfd __user *, unsigned int,
struct timespec __user *, const sigset_t __user *,
size_t);

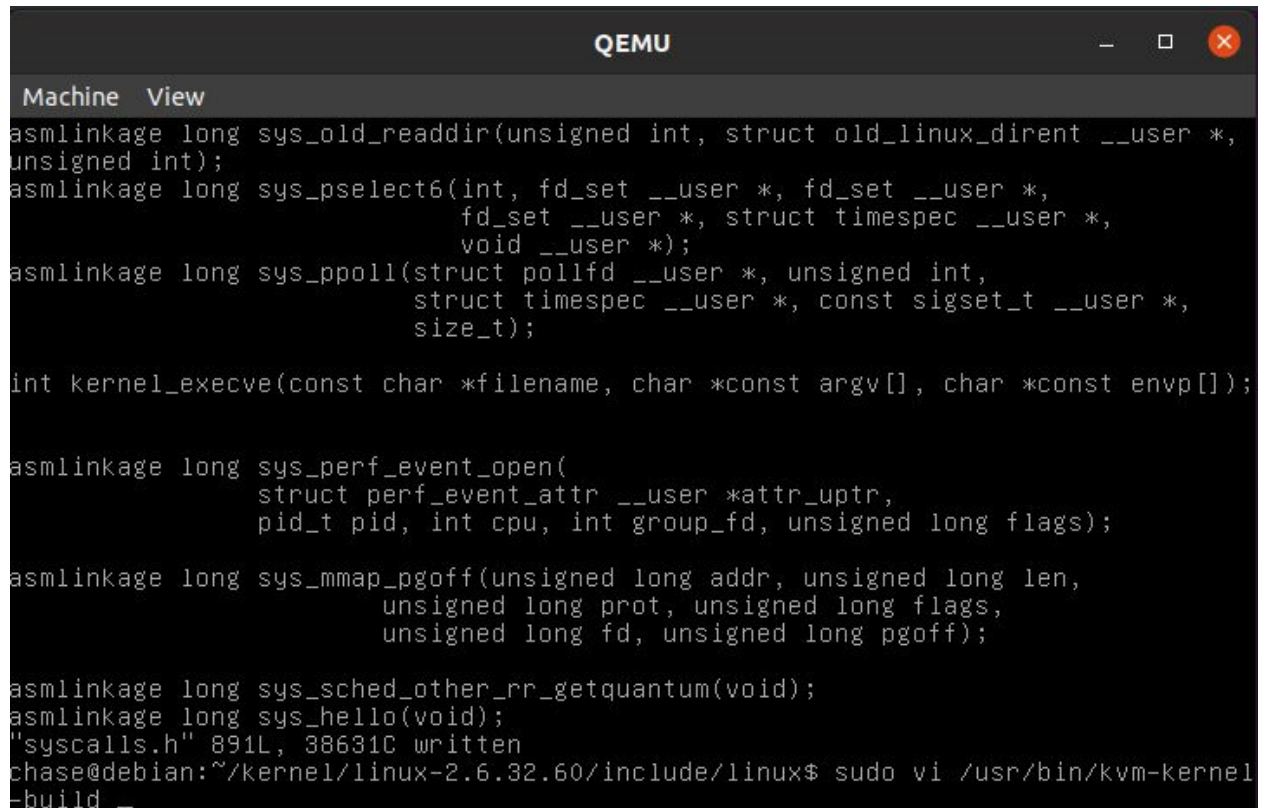
int kernel_execve(const char *filename, char *const argv[], char *const envp[]);

asmlinkage long sys_perf_event_open(
struct perf_event_attr __user *attr_uptr,
pid_t pid, int cpu, int group_fd, unsigned long flags);

asmlinkage long sys_mmap_pgoff(unsigned long addr, unsigned long len,
unsigned long prot, unsigned long flags,
unsigned long fd, unsigned long pgoff);

asmlinkage long sys_sched_other_rr_getquantum(void);
asmlinkage long sys_hello(void);_
-- INSERT --
890,33 99%
```

15.) Modified syscalls.h and added the function sys_hello(void);



A screenshot of a QEMU terminal window. The window title is "QEMU". The terminal displays kernel source code for system calls, including `sys_old_readdir`, `sys_pselect6`, `sys_ppoll`, `kernel_execve`, `sys_perf_event_open`, `sys_mmap_pgoff`, `sys_sched_other_rr_getquantum`, and `sys_hello`. At the bottom, a prompt shows the user `chase@debian` in the directory `~/kernel/linux-2.6.32.60/include/linux`, having executed `sudo vi /usr/bin/kvm-kernel-build _`.

```
Machine  View
asmlinkage long sys_old_readdir(unsigned int, struct old_linux_dirent __user *,
unsigned int);
asmlinkage long sys_pselect6(int, fd_set __user *, fd_set __user *,
                             fd_set __user *, struct timespec __user *,
                             void __user *);
asmlinkage long sys_ppoll(struct pollfd __user *, unsigned int,
                          struct timespec __user *, const sigset_t __user *,
                          size_t);

int kernel_execve(const char *filename, char *const argv[], char *const envp[]);

asmlinkage long sys_perf_event_open(
    struct perf_event_attr __user *attr_uptr,
    pid_t pid, int cpu, int group_fd, unsigned long flags);

asmlinkage long sys_mmap_pgoff(unsigned long addr, unsigned long len,
                                unsigned long prot, unsigned long flags,
                                unsigned long fd, unsigned long pgoff);

asmlinkage long sys_sched_other_rr_getquantum(void);
asmlinkage long sys_hello(void);
'syscalls.h' 891L, 38631C written
chase@debian:~/kernel/linux-2.6.32.60/include/linux$ sudo vi /usr/bin/kvm-kernel
-build _
```

16.) Opened kvm-kernel-build script

The screenshot shows a QEMU window with a terminal. The terminal has a title bar with 'QEMU' and standard window controls. Below the title bar is a header with 'Machine' and 'View'. The terminal content is as follows:

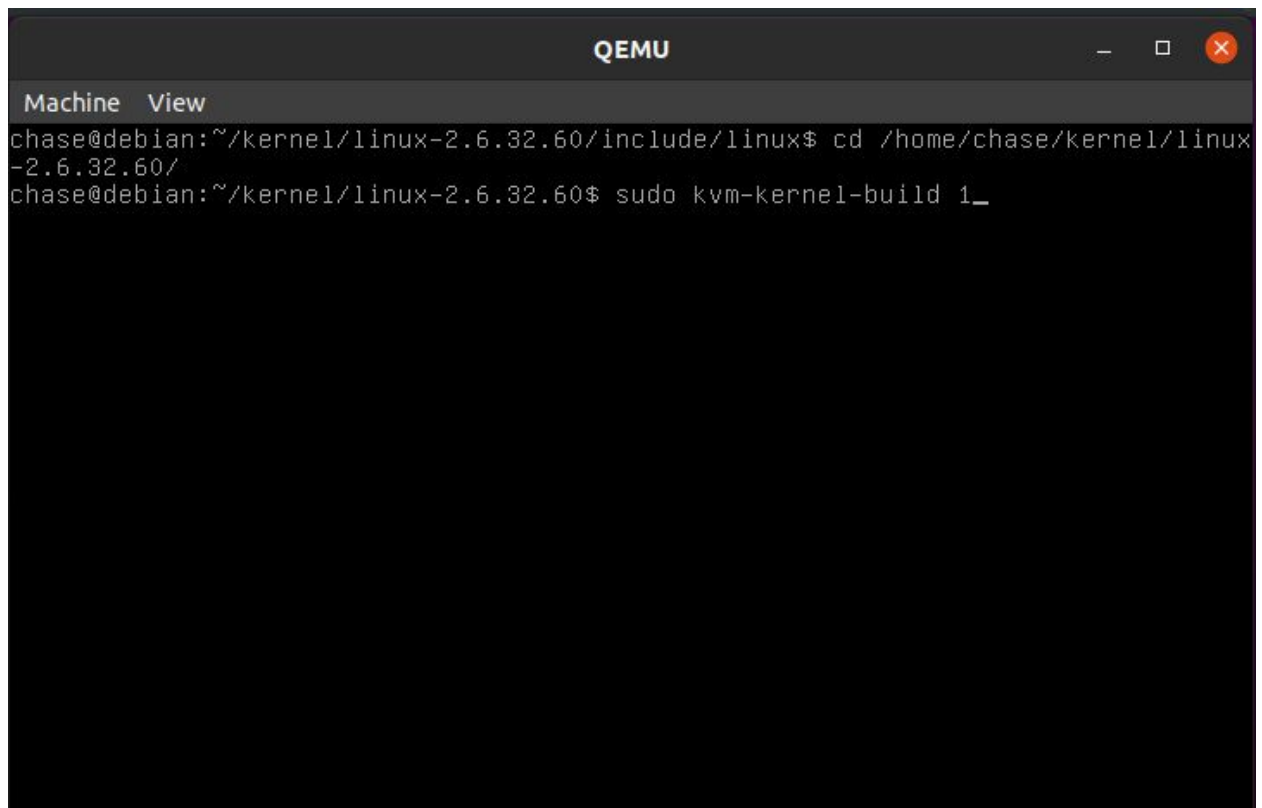
```

1 #!/bin/sh
2 rev=$1
3 if [ -z "$rev" ]; then
4     echo "Usage: build64 <revision>"
5     exit 1
6 fi
7 make-kpkg -- 2 --rootcmd fakeroot --initrd --revision=$rev kernel_image 2>&1

```

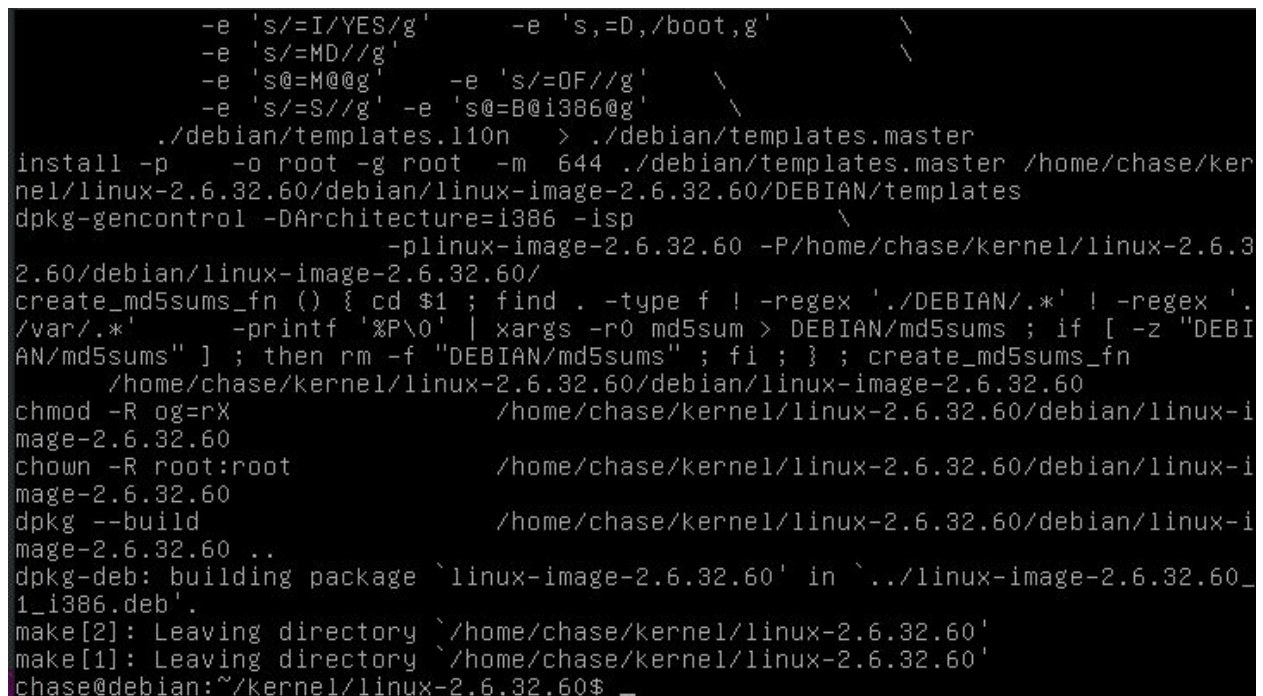
At the bottom of the window, there is a status bar with the text 'INSERT --' on the left, '7,15' in the center, and 'All' on the right.

17.) Changed build script to include a -j flag and a 2 value



```
Machine View
chase@debian:~/kernel/linux-2.6.32.60/include/linux$ cd /home/chase/kernel/linux-2.6.32.60/
chase@debian:~/kernel/linux-2.6.32.60$ sudo kvm-kernel-build 1_
```

18.) Built the kernel.



```
-e 's/=I/YES/g' -e 's,=D,/boot,g' \
-e 's/=MD//g' \
-e 's@=M@@g' -e 's/=OF//g' \
-e 's/=S//g' -e 's@=B@i386@g' \
./debian/templates.l10n > ./debian/templates.master
install -p -o root -g root -m 644 ./debian/templates.master /home/chase/kernel/linux-2.6.32.60/debian/linux-image-2.6.32.60/DEBIAN/templates
dpkg-gencontrol -DArchitecture=i386 -isp \
-plinux-image-2.6.32.60 -P/home/chase/kernel/linux-2.6.32.60/debian/linux-image-2.6.32.60/
create_md5sums_fn () { cd $1 ; find . -type f ! -regex './DEBIAN/.*' ! -regex './var/.*' -printf '%P\n' | xargs -r0 md5sum > DEBIAN/md5sums ; if [ -z "DEBIAN/md5sums" ] ; then rm -f "DEBIAN/md5sums" ; fi ; } ; create_md5sums_fn /home/chase/kernel/linux-2.6.32.60/debian/linux-image-2.6.32.60
chmod -R og=rX /home/chase/kernel/linux-2.6.32.60/debian/linux-image-2.6.32.60
chown -R root:root /home/chase/kernel/linux-2.6.32.60/debian/linux-image-2.6.32.60
dpkg --build /home/chase/kernel/linux-2.6.32.60/debian/linux-image-2.6.32.60 ..
dpkg-deb: building package `linux-image-2.6.32.60' in `../linux-image-2.6.32.60_1_i386.deb'.
make[2]: Leaving directory `/home/chase/kernel/linux-2.6.32.60'
make[1]: Leaving directory `/home/chase/kernel/linux-2.6.32.60'
chase@debian:~/kernel/linux-2.6.32.60$ _
```

19.) Output of the successful kernel build

```
Machine View
Selecting previously deselected package linux-image-2.6.32.60.
(Reading database ... 23905 files and directories currently installed.)
Unpacking linux-image-2.6.32.60 (from linux-image-2.6.32.60_1_i386.deb) ...
Done.
Setting up linux-image-2.6.32.60 (1) ...
Running depmod.
Examining /etc/kernel/postinst.d.
run-parts: executing /etc/kernel/postinst.d/initramfs-tools 2.6.32.60 /boot/vmlinuz-2.6.32.60
update-initramfs: Generating /boot/initrd.img-2.6.32.60
run-parts: executing /etc/kernel/postinst.d/zz-update-grub 2.6.32.60 /boot/vmlinuz-2.6.32.60
Generating grub.cfg ...
Found linux image: /boot/vmlinuz-2.6.32.60
Found initrd image: /boot/initrd.img-2.6.32.60
Found linux image: /boot/vmlinuz-2.6.32-5-686
Found initrd image: /boot/initrd.img-2.6.32-5-686
done

[/home/chase/kernel]
root@debian$ ls
linux-2.6.32.60/  linux-image-2.6.32.60_1_i386.deb

[/home/chase/kernel]
root@debian$
```

20.) Output of the dpkg command to install the kernel to the vm

```
SeaBIOS (version 1.13.0-1ubuntu1)
Decompressing Linux... Parsing ELF... done.
Booting the kernel.
iPXE (http://ipxe.org) 00:03.0 CA00 PCI2.10 PnP PMM+7FF8CB00+7FECCB00 CA00
Debian GNU/Linux 6.0 debian tty1

debian login: root
Password: om Hard Disk...
Last login: Fri Sep 25 10:22:07 CDT 2020 on tty1
Linux debian 2.6.32.60 #2 SMP Fri Sep 25 11:23:32 CDT 2020 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

[~]
root@debian$ uname -a
Linux debian 2.6.32.60 #2 SMP Fri Sep 25 11:23:32 CDT 2020 i686 GNU/Linux

[~]
root@debian$
```

21.) After rebooting and using uname -a to check correct kernel


```
Machine view
#include <sys/syscall.h>
#include <unistd.h>
#include <linux/kernel.h>
int main()
{
    long int syscall_val = syscall(338);
    printf("System call sys_hello returned %ld\n",syscall_val);
    return 0;
}

"test_syscall.c" [New] 10L, 215C written
chase@debian:~$
```

22.) Test_syscall.c program

```
chase@debian:~$ gcc test_syscall.c -o test_syscall
chase@debian:~$ ./test_syscall
System call sys_hello returned 100
chase@debian:~$
```

23.) Output of test_syscall.c program

```
chase@debian:~$ gcc test_syscall.c -o test_syscall
chase@debian:~$ ./test_syscall
System call sys_hello returned 100
chase@debian:~$ dmesg | tail -5
[ 16.094699] loop: module loaded
[ 19.589077] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: R
X
[ 19.591971] ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 19.592933] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[ 317.500907] Hello World!
chase@debian:~$ _
```

24.) The last 5 lines of the kernel including the "Hello World!" I had modified