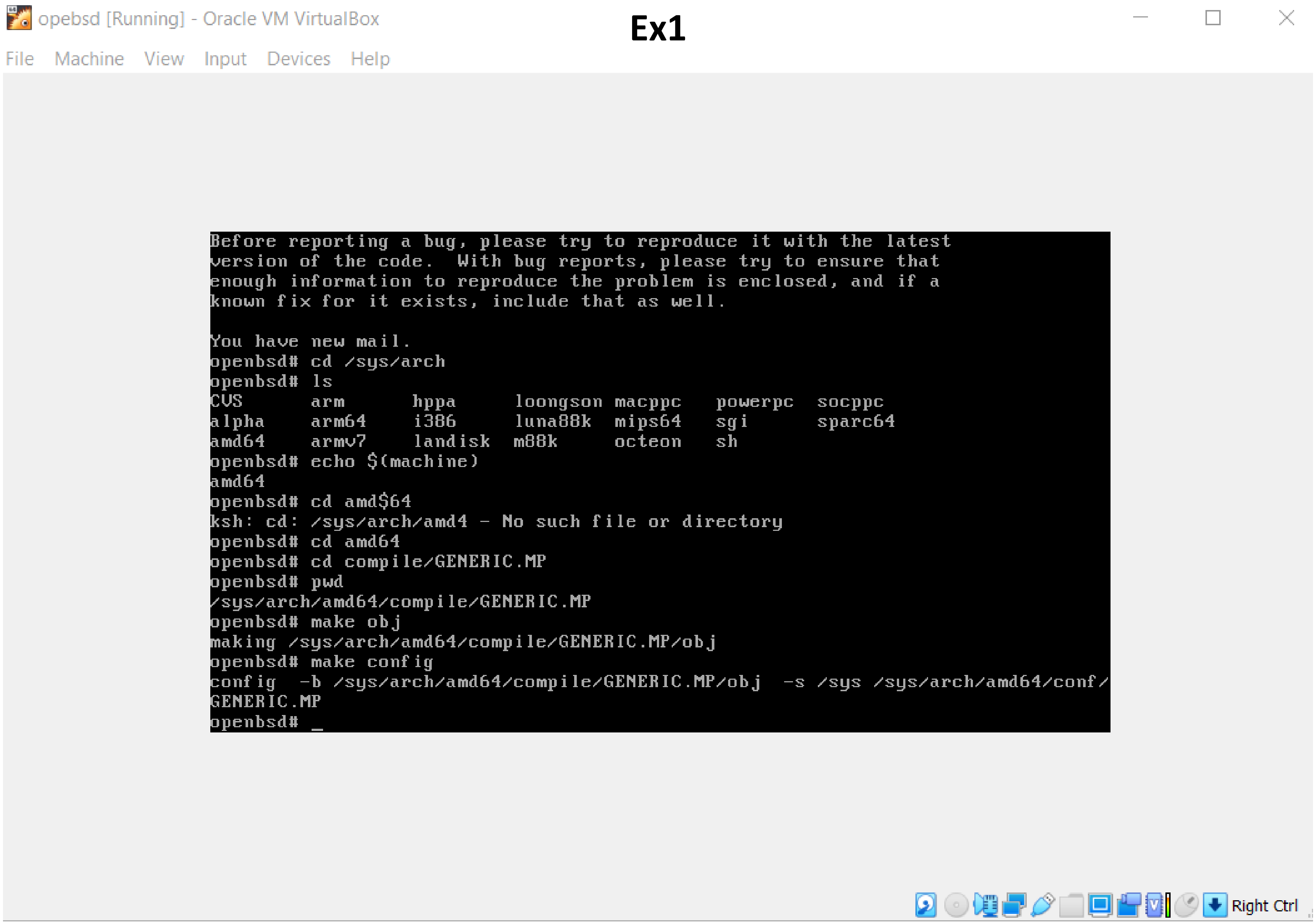
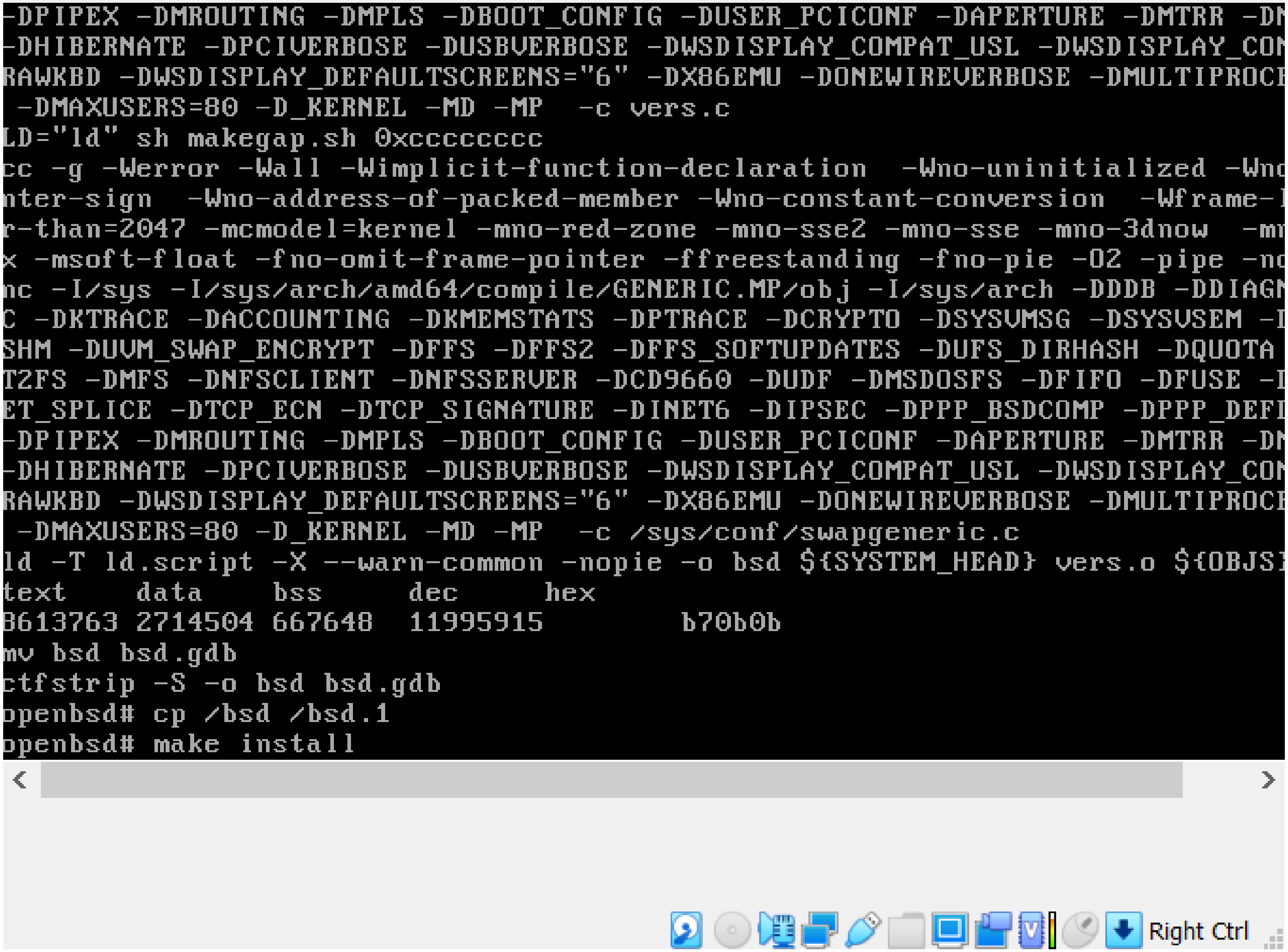
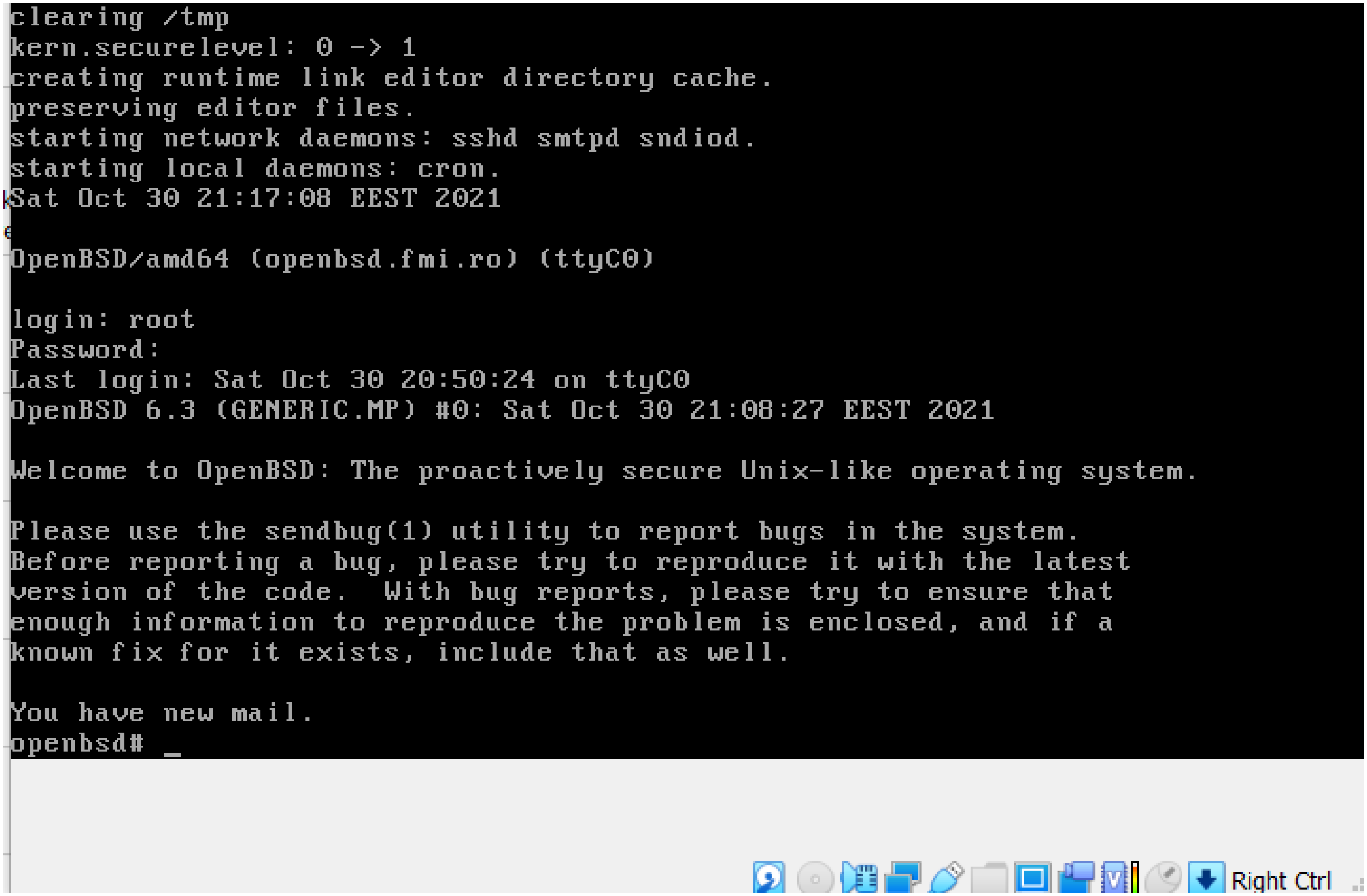
Ex1



```
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

You have new mail.
openbsd# cd /sys/arch
openbsd# ls
CVS      arm      hppa     loongson macppc   powerpc  socppc
alpha    arm64    i386     luna88k  mips64   sgi      sparc64
amd64    armv7    landisk  m88k     octeon   sh
openbsd# echo $(machine)
amd64
openbsd# cd amd$64
ksh: cd: /sys/arch/amd4 - No such file or directory
openbsd# cd amd64
openbsd# cd compile/GENERIC.MP
openbsd# pwd
/sys/arch/amd64/compile/GENERIC.MP
openbsd# make obj
making /sys/arch/amd64/compile/GENERIC.MP/obj
openbsd# make config
config  -b /sys/arch/amd64/compile/GENERIC.MP/obj  -s /sys /sys/arch/amd64/conf/
GENERIC.MP
openbsd# _
```



```
-DPIPEX -DMROUTING -DMPLS -DBOOT_CONFIG -DUSER_PCICONF -DAPERTURE -DMTRR -DN
-DHIBERNATE -DPCIVERBOSE -DUSBVERBOSE -DWSDISPLAY_COMPAT_USL -DWSDISPLAY_COM
RAWKBD -DWSDISPLAY_DEFAULTSCREENS="6" -DX86EMU -DONEWIREVERBOSE -DMULTIPROCE
 -DMAXUSERS=80 -D_KERNEL -MD -MP  -c vers.c
LD="ld" sh makegap.sh 0xcccccccc
cc -g -Werror -Wall -Wimplicit-function-declaration  -Wno-uninitialized -Wno
nter-sign  -Wno-address-of-packed-member -Wno-constant-conversion  -Wframe-l
r-than=2047 -mcmodel=kernel -mno-red-zone -mno-sse2 -mno-sse -mno-3dnow  -mn
x -msoft-float -fno-omit-frame-pointer -ffreestanding -fno-pie -O2 -pipe -no
nc -I/sys -I/sys/arch/amd64/compile/GENERIC.MP/obj -I/sys/arch -DDDB -DDIAGN
C -DKTRACE -DACCOUNTING -DKMEMSTATS -DPTRACE -DCRYPTO -DSYSVMSG -DSYSVSEM -D
SHM -DUVM_SWAP_ENCRYPT -DFFS -DFFS2 -DFFS_SOFTUPDATES -DUFS_DIRHASH -DQUOTA
T2FS -DMFS -DNFSCLIENT -DNFSSERVER -DCD9660 -DUDF -DMSDOSFS -DFIFO -DFUSE -D
ET_SPLICE -DTCP_ECN -DTCP_SIGNATURE -DINET6 -DIPSEC -DPPP_BSDCOMP -DPPP_DEFL
-DPIPEX -DMROUTING -DMPLS -DBOOT_CONFIG -DUSER_PCICONF -DAPERTURE -DMTRR -DN
-DHIBERNATE -DPCIVERBOSE -DUSBVERBOSE -DWSDISPLAY_COMPAT_USL -DWSDISPLAY_COM
RAWKBD -DWSDISPLAY_DEFAULTSCREENS="6" -DX86EMU -DONEWIREVERBOSE -DMULTIPROCE
 -DMAXUSERS=80 -D_KERNEL -MD -MP  -c /sys/conf/swapgeneric.c
ld -T ld.script -X --warn-common -nopie -o bsd ${SYSTEM_HEAD} vers.o ${OBJS}
text    data    bss     dec     hex
8613763 2714504 667648  11995915        b70b0b
mv bsd bsd.gdb
ctfstrip -S -o bsd bsd.gdb
openbsd# cp /bsd /bsd.1
openbsd# make install
```

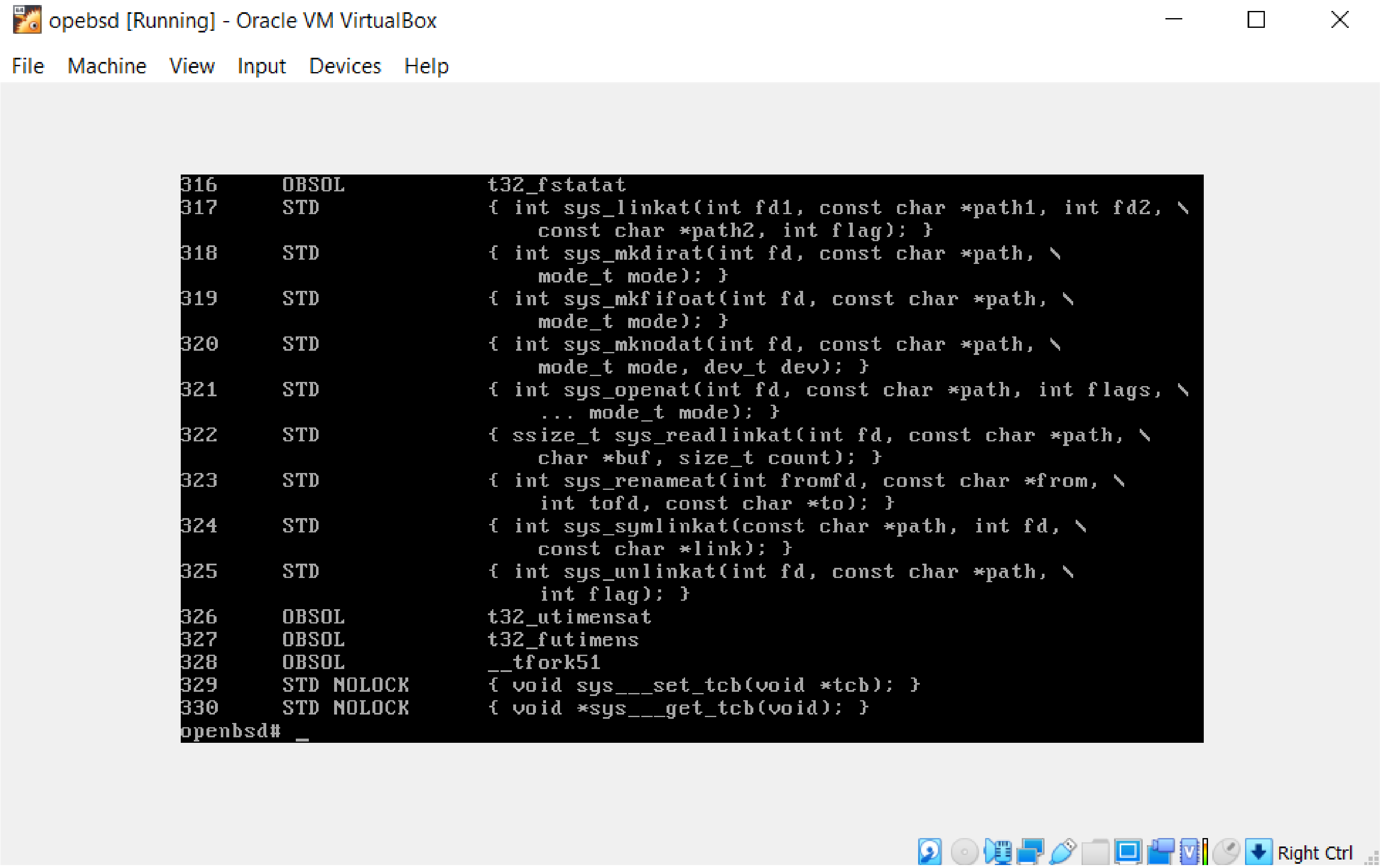


```
clearing /tmp
kern.securelevel: 0 -> 1
creating runtime link editor directory cache.
preserving editor files.
starting network daemons: sshd smtpd sndiod.
starting local daemons: cron.
Sat Oct 30 21:17:08 EEST 2021

OpenBSD/amd64 (openbsd.fmi.ro) (ttyC0)

login: root
Password:
Last login: Sat Oct 30 20:50:24 on ttyC0
OpenBSD 6.3 (GENERIC.MP) #0: Sat Oct 30 21:08:27 EEST 2021

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

You have new mail.
openbsd# _
```

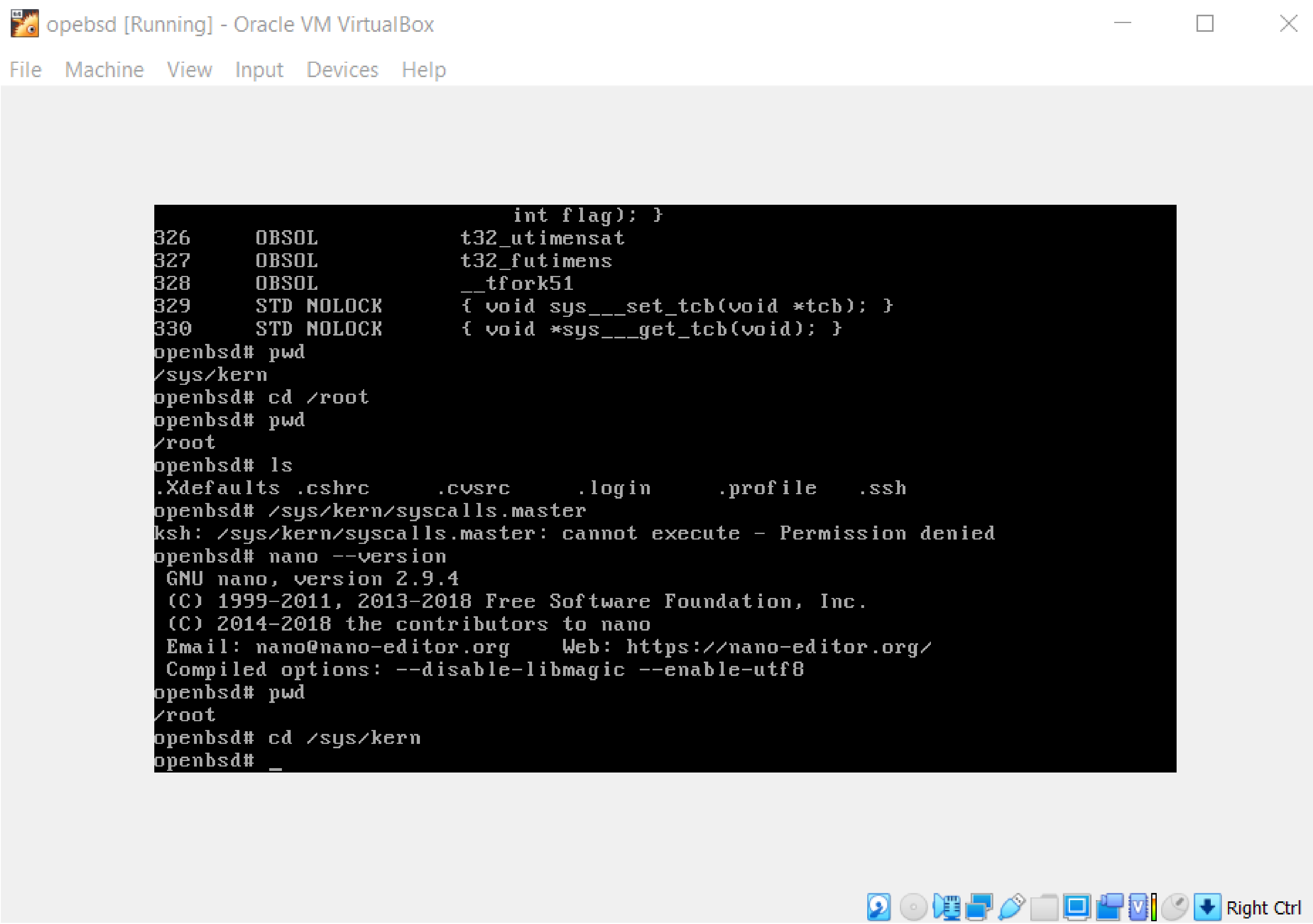
EX2

#cd /sys/kern

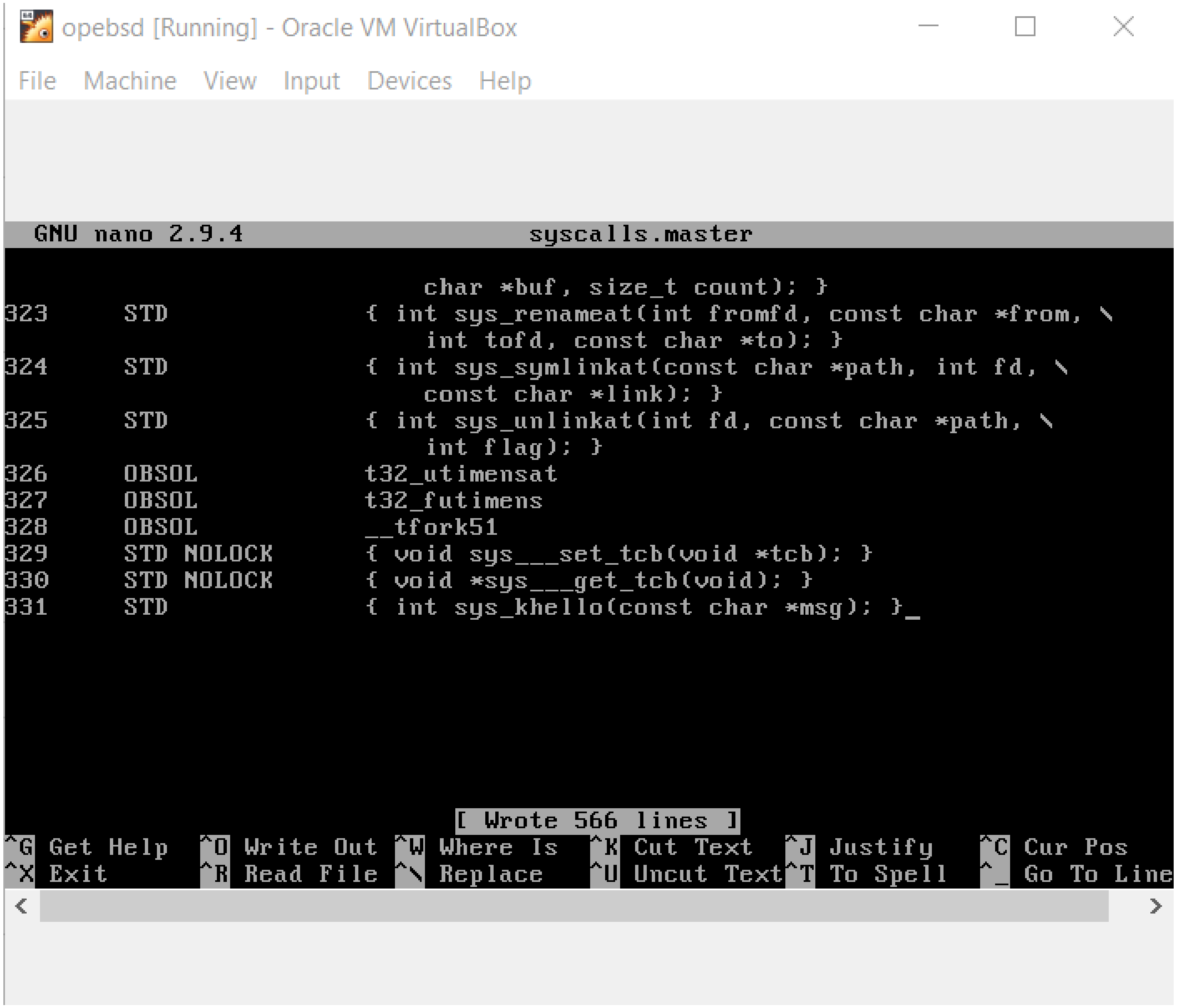
# cat syscalls.master



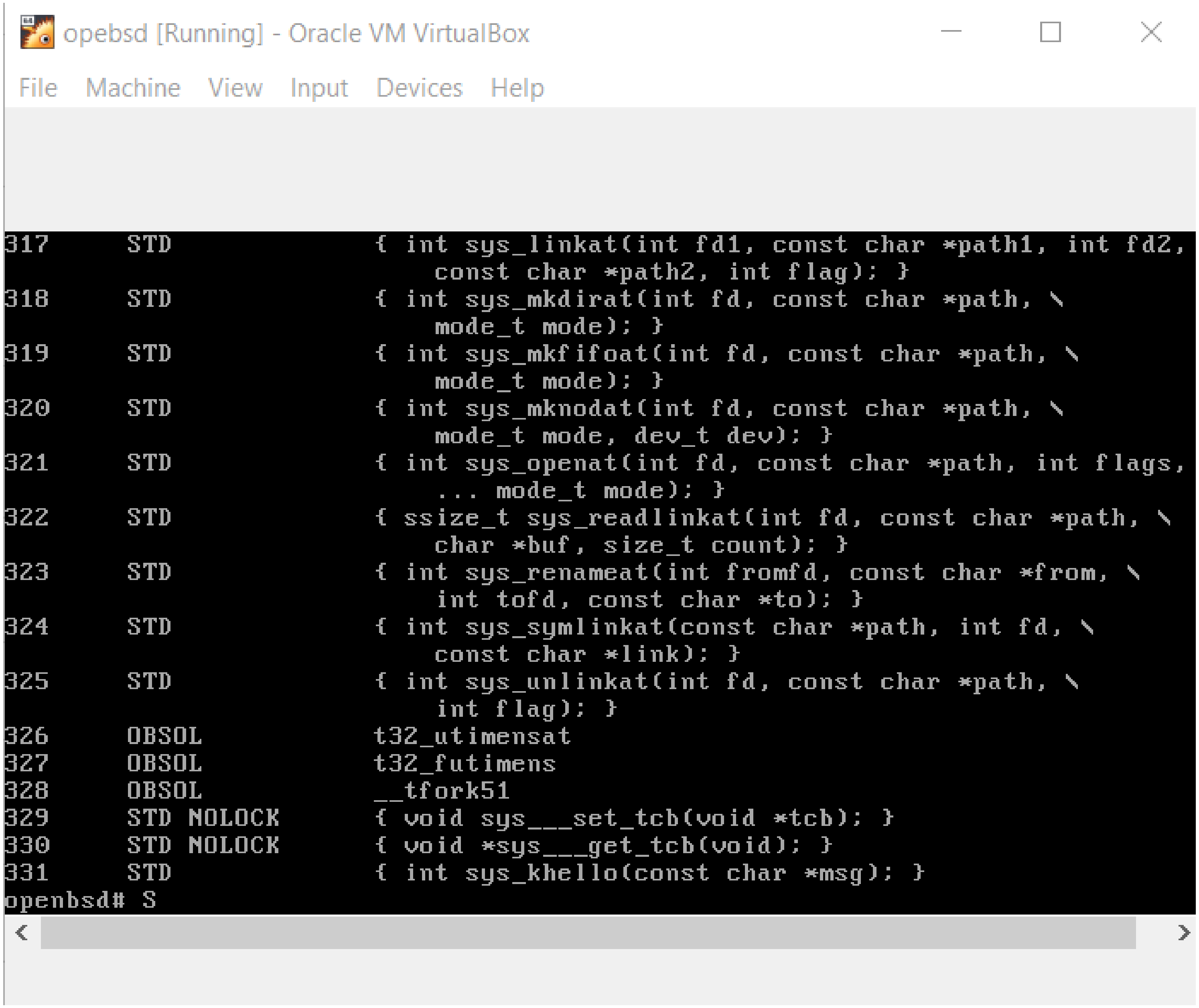
```
316     OBSOL           t32_fstatat
317     STD             { int sys_linkat(int fd1, const char *path1, int fd2, \
                            const char *path2, int flag); }
318     STD             { int sys_mkdirat(int fd, const char *path, \
                            mode_t mode); }
319     STD             { int sys_mkfifoat(int fd, const char *path, \
                            mode_t mode); }
320     STD             { int sys_mknodat(int fd, const char *path, \
                            mode_t mode, dev_t dev); }
321     STD             { int sys_openat(int fd, const char *path, int flags, \
                            ... mode_t mode); }
322     STD             { ssize_t sys_readlinkat(int fd, const char *path, \
                            char *buf, size_t count); }
323     STD             { int sys_renameat(int fromfd, const char *from, \
                            int tofd, const char *to); }
324     STD             { int sys_symlinkat(const char *path, int fd, \
                            const char *link); }
325     STD             { int sys_unlinkat(int fd, const char *path, \
                            int flag); }
326     OBSOL           t32_utimensat
327     OBSOL           t32_futimens
328     OBSOL           __tfork51
329     STD NOLOCK      { void sys___set_tcb(void *tcb); }
330     STD NOLOCK      { void *sys___get_tcb(void); }
openbsd# _
```



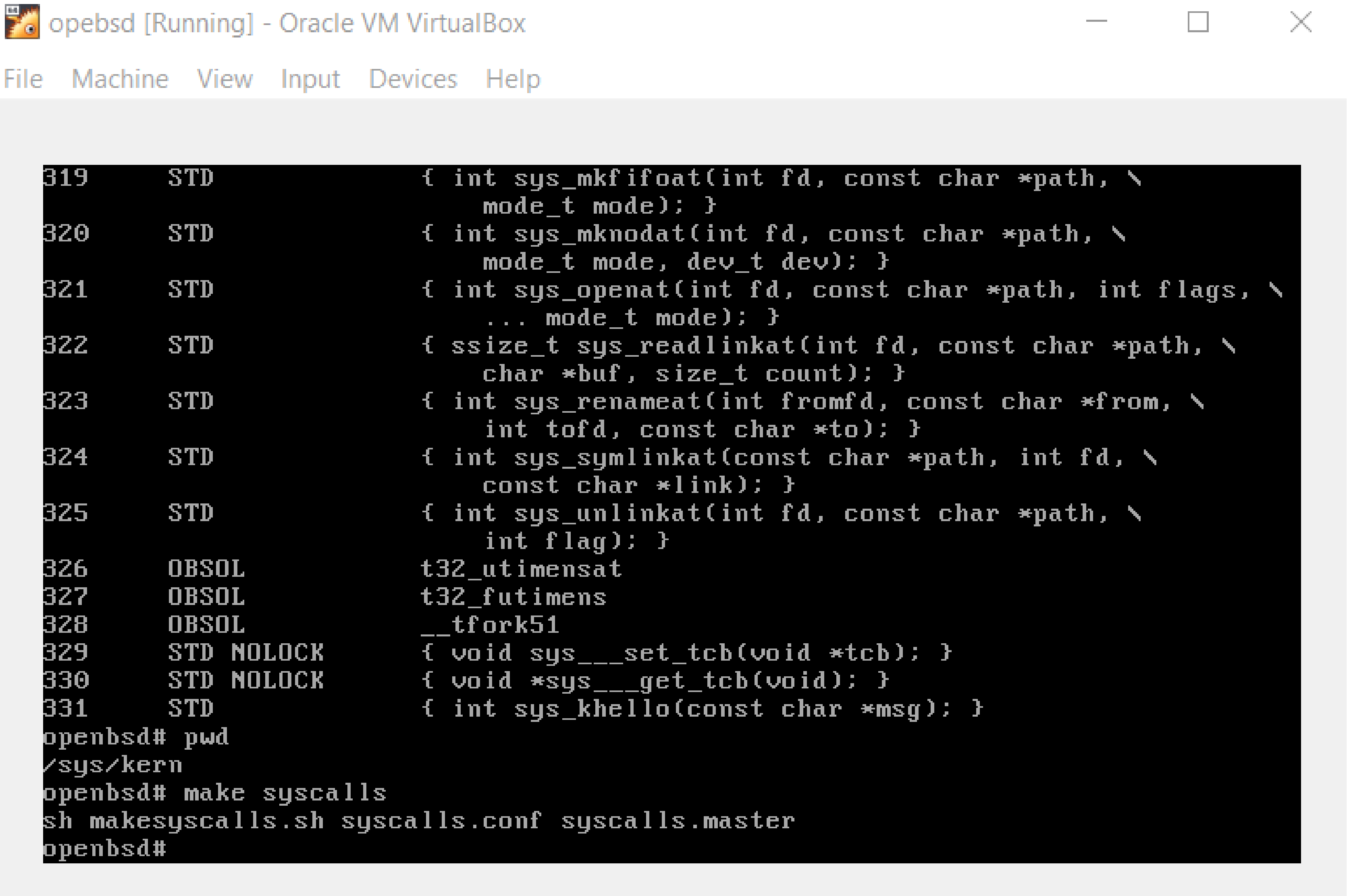
```
                            int flag); }
326     OBSOL           t32_utimensat
327     OBSOL           t32_futimens
328     OBSOL           __tfork51
329     STD NOLOCK      { void sys___set_tcb(void *tcb); }
330     STD NOLOCK      { void *sys___get_tcb(void); }
openbsd# pwd
/sys/kern
openbsd# cd /root
openbsd# pwd
/root
openbsd# ls
.Xdefaults .cshrc     .cvsrc     .login     .profile   .ssh
openbsd# /sys/kern/syscalls.master
ksh: /sys/kern/syscalls.master: cannot execute - Permission denied
openbsd# nano --version
 GNU nano, version 2.9.4
 (C) 1999-2011, 2013-2018 Free Software Foundation, Inc.
 (C) 2014-2018 the contributors to nano
 Email: nano@nano-editor.org    Web: https://nano-editor.org/
 Compiled options: --disable-libmagic --enable-utf8
openbsd# pwd
/root
openbsd# cd /sys/kern
openbsd# _
```



```
 GNU nano 2.9.4                            syscalls.master

                            char *buf, size_t count); }
323     STD                 { int sys_renameat(int fromfd, const char *from, \
                                int tofd, const char *to); }
324     STD                 { int sys_symlinkat(const char *path, int fd, \
                                const char *link); }
325     STD                 { int sys_unlinkat(int fd, const char *path, \
                                int flag); }
326     OBSOL               t32_utimensat
327     OBSOL               t32_futimens
328     OBSOL               __tfork51
329     STD NOLOCK          { void sys___set_tcb(void *tcb); }
330     STD NOLOCK          { void *sys___get_tcb(void); }
331     STD                 { int sys_khello(const char *msg); }_




                                  [ Wrote 566 lines ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text^T To Spell       ^_ Go To Line
```

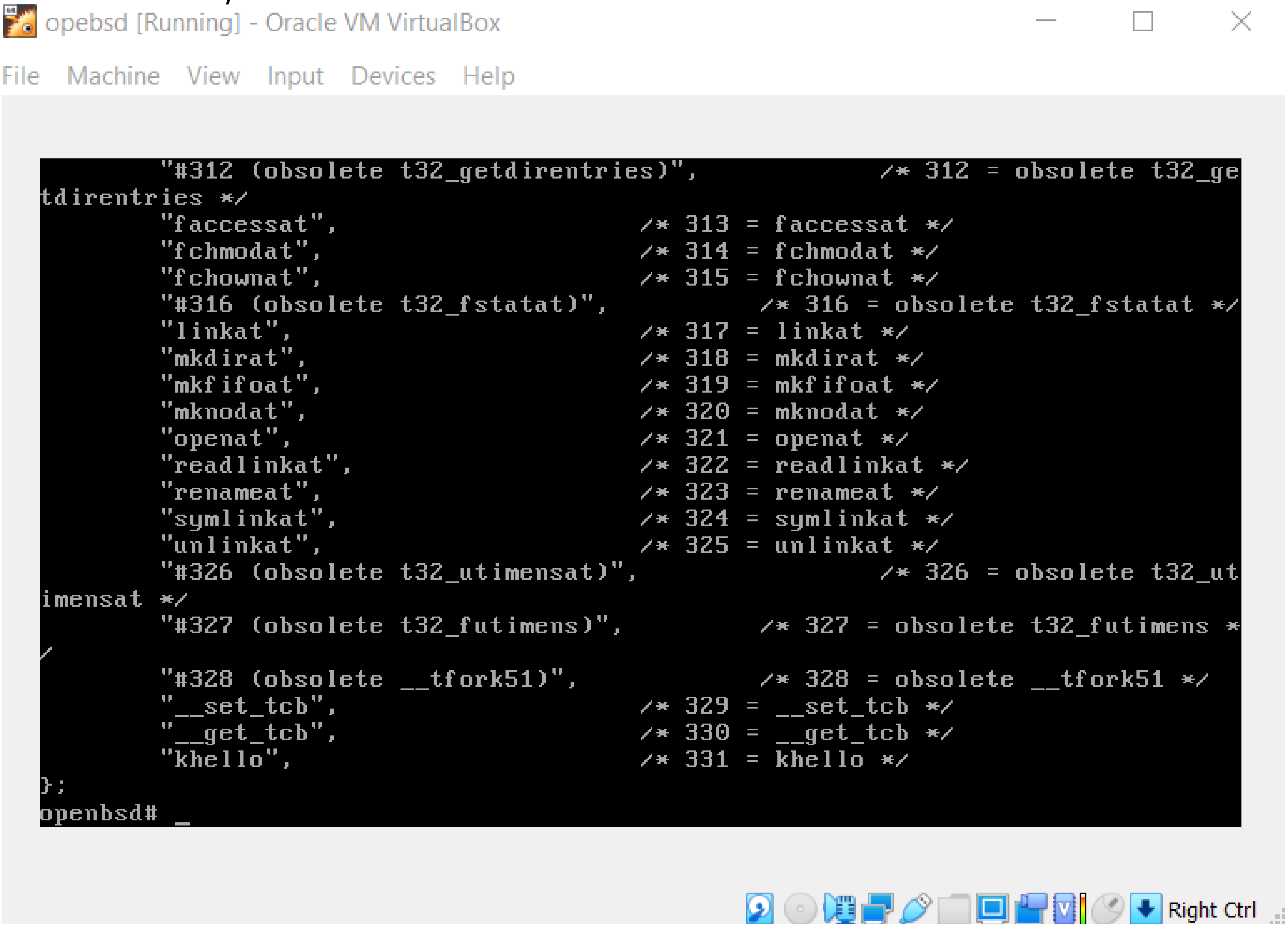


```
317     STD             { int sys_linkat(int fd1, const char *path1, int fd2,
                            const char *path2, int flag); }
318     STD             { int sys_mkdirat(int fd, const char *path, \
                            mode_t mode); }
319     STD             { int sys_mkfifoat(int fd, const char *path, \
                            mode_t mode); }
320     STD             { int sys_mknodat(int fd, const char *path, \
                            mode_t mode, dev_t dev); }
321     STD             { int sys_openat(int fd, const char *path, int flags,
                            ... mode_t mode); }
322     STD             { ssize_t sys_readlinkat(int fd, const char *path, \
                            char *buf, size_t count); }
323     STD             { int sys_renameat(int fromfd, const char *from, \
                            int tofd, const char *to); }
324     STD             { int sys_symlinkat(const char *path, int fd, \
                            const char *link); }
325     STD             { int sys_unlinkat(int fd, const char *path, \
                            int flag); }
326     OBSOL           t32_utimensat
327     OBSOL           t32_futimens
328     OBSOL           __tfork51
329     STD NOLOCK      { void sys___set_tcb(void *tcb); }
330     STD NOLOCK      { void *sys___get_tcb(void); }
331     STD             { int sys_khello(const char *msg); }
openbsd# S
```

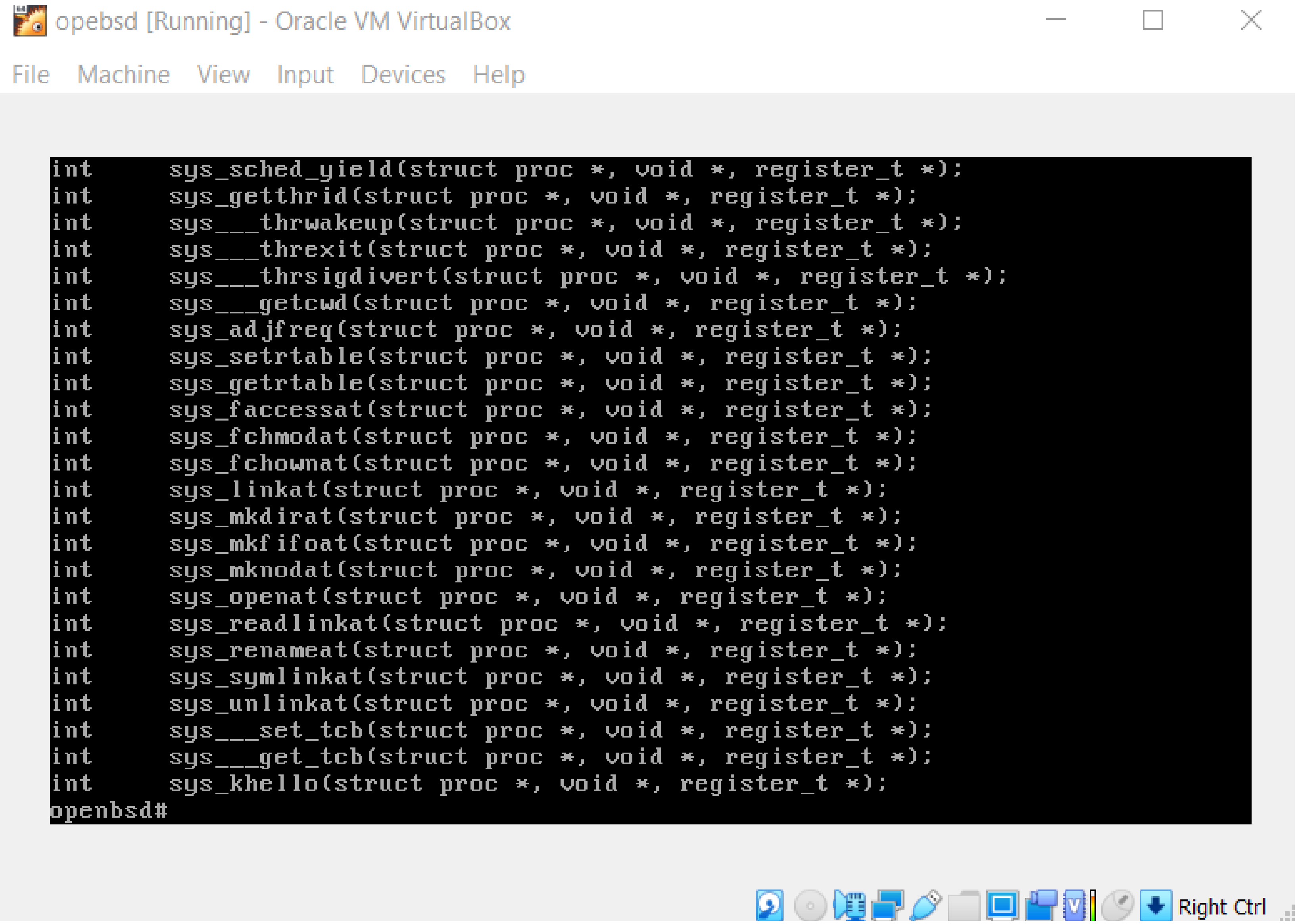


```
319     STD                     { int sys_mkfifoat(int fd, const char *path, \
                                    mode_t mode); }
320     STD                     { int sys_mknodat(int fd, const char *path, \
                                    mode_t mode, dev_t dev); }
321     STD                     { int sys_openat(int fd, const char *path, int flags, \
                                    ... mode_t mode); }
322     STD                     { ssize_t sys_readlinkat(int fd, const char *path, \
                                    char *buf, size_t count); }
323     STD                     { int sys_renameat(int fromfd, const char *from, \
                                    int tofd, const char *to); }
324     STD                     { int sys_symlinkat(const char *path, int fd, \
                                    const char *link); }
325     STD                     { int sys_unlinkat(int fd, const char *path, \
                                    int flag); }
326     OBSOL                   t32_utimensat
327     OBSOL                   t32_futimens
328     OBSOL                   __tfork51
329     STD NOLOCK              { void sys___set_tcb(void *tcb); }
330     STD NOLOCK              { void *sys___get_tcb(void); }
331     STD                     { int sys_khello(const char *msg); }
openbsd# pwd
/sys/kern
openbsd# make syscalls
sh makesyscalls.sh syscalls.conf syscalls.master
openbsd#
```

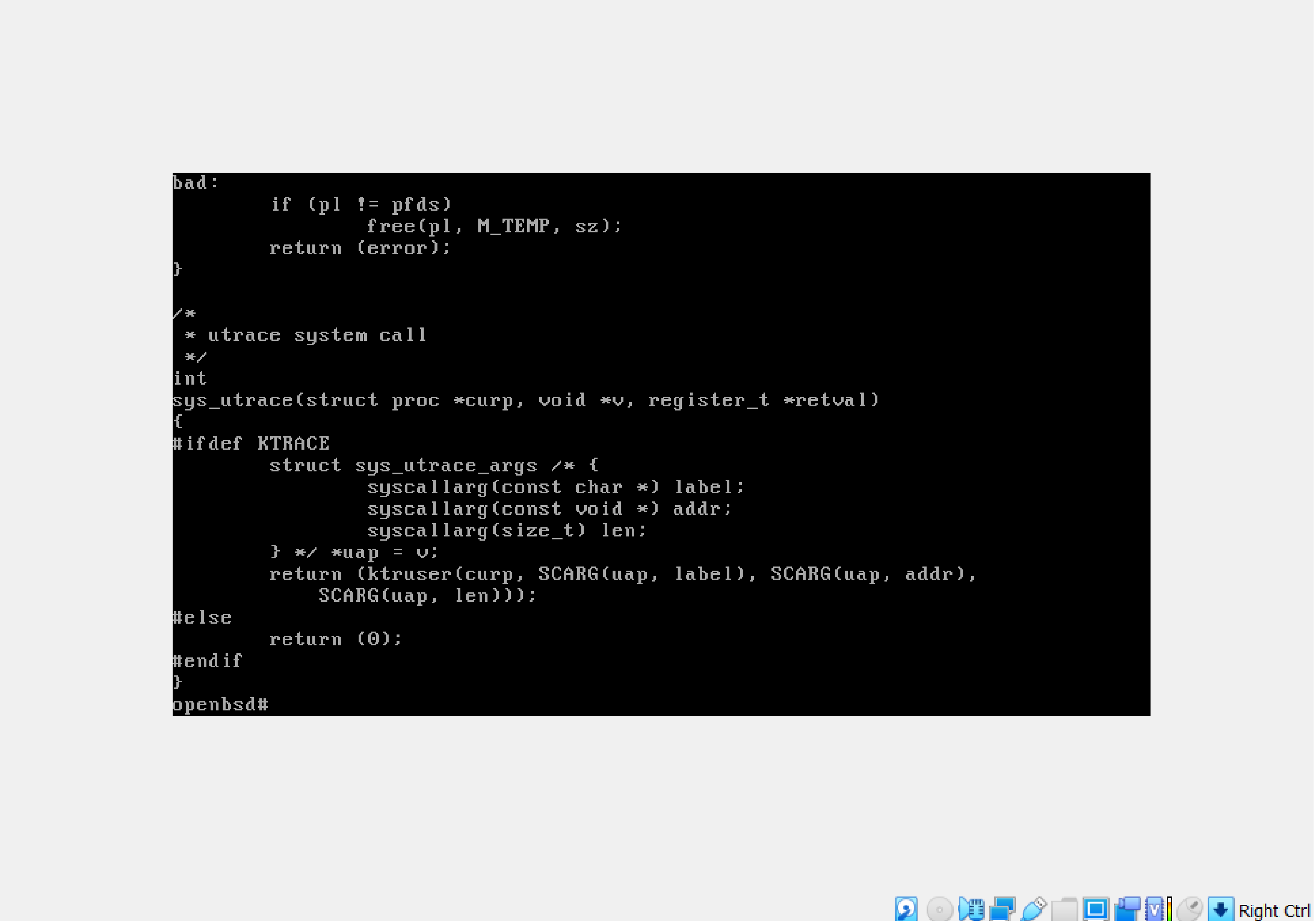
dupa ce am dat #cat syscallss.c



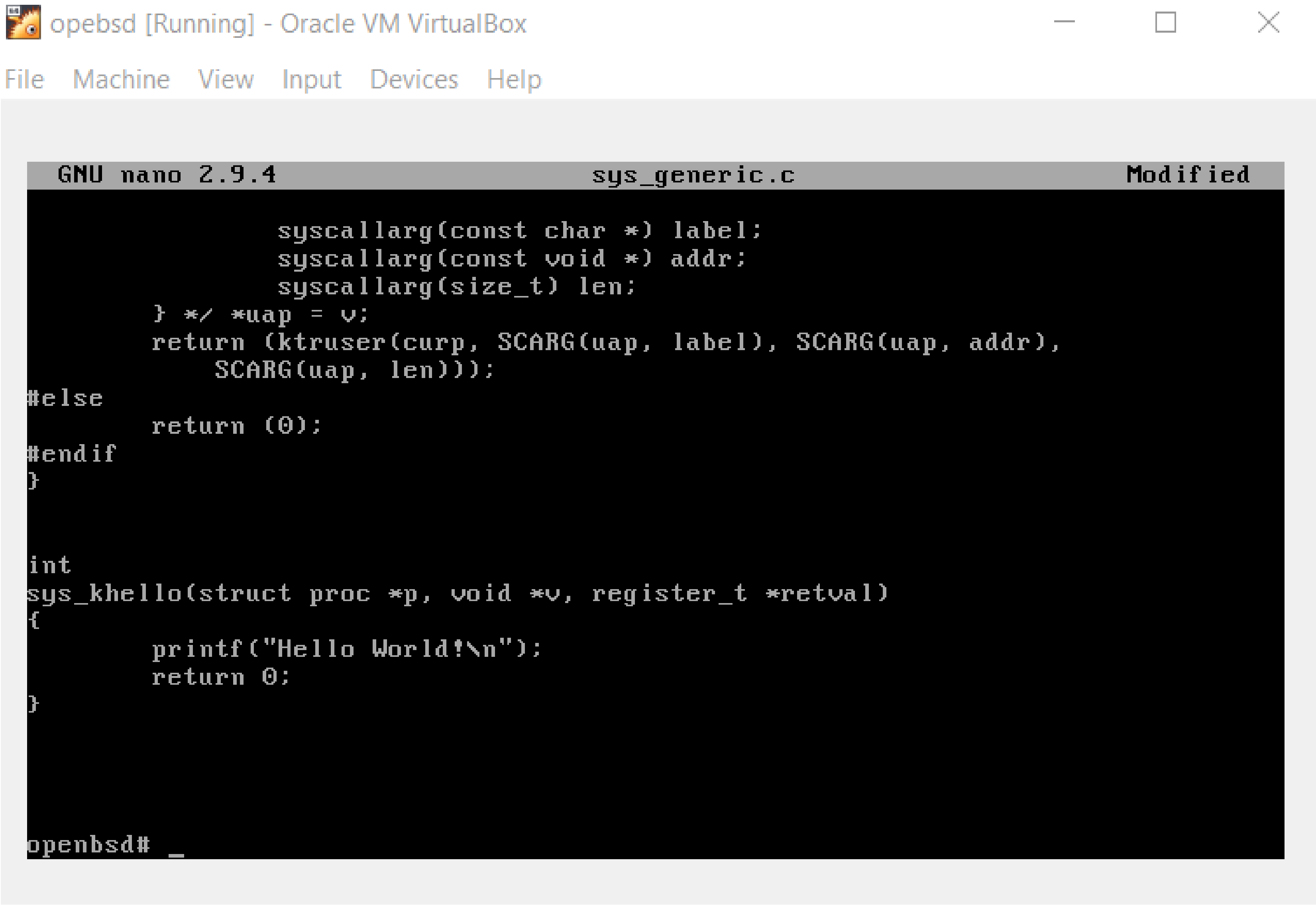
```
        "#312 (obsolete t32_getdirentries)",            /* 312 = obsolete t32_ge
tdirentries */
        "faccessat",                    /* 313 = faccessat */
        "fchmodat",                     /* 314 = fchmodat */
        "fchownat",                     /* 315 = fchownat */
        "#316 (obsolete t32_fstatat)",          /* 316 = obsolete t32_fstatat */
        "linkat",                       /* 317 = linkat */
        "mkdirat",                      /* 318 = mkdirat */
        "mkfifoat",                     /* 319 = mkfifoat */
        "mknodat",                      /* 320 = mknodat */
        "openat",                       /* 321 = openat */
        "readlinkat",                   /* 322 = readlinkat */
        "renameat",                     /* 323 = renameat */
        "symlinkat",                    /* 324 = symlinkat */
        "unlinkat",                     /* 325 = unlinkat */
        "#326 (obsolete t32_utimensat)",                /* 326 = obsolete t32_ut
imensat */
        "#327 (obsolete t32_futimens)",         /* 327 = obsolete t32_futimens *
/

        "#328 (obsolete __tfork51)",            /* 328 = obsolete __tfork51 */
        "__set_tcb",                    /* 329 = __set_tcb */
        "__get_tcb",                    /* 330 = __get_tcb */
        "khello",                       /* 331 = khello */
};
openbsd# _
```



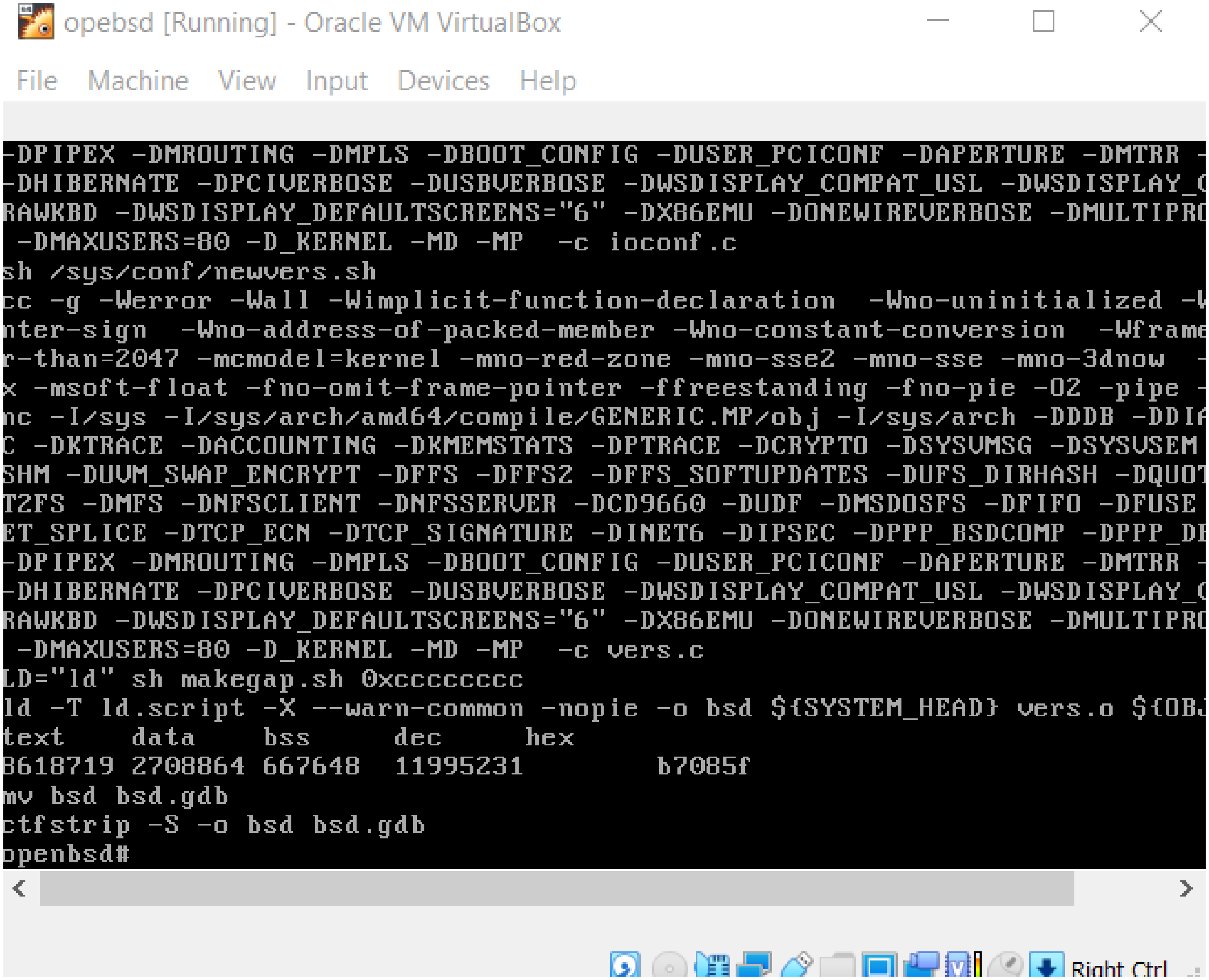
```
int     sys_sched_yield(struct proc *, void *, register_t *);
int     sys_getthrid(struct proc *, void *, register_t *);
int     sys___thrwakeup(struct proc *, void *, register_t *);
int     sys___threxit(struct proc *, void *, register_t *);
int     sys___thrsigdivert(struct proc *, void *, register_t *);
int     sys___getcwd(struct proc *, void *, register_t *);
int     sys_adjfreq(struct proc *, void *, register_t *);
int     sys_setrtable(struct proc *, void *, register_t *);
int     sys_getrtable(struct proc *, void *, register_t *);
int     sys_faccessat(struct proc *, void *, register_t *);
int     sys_fchmodat(struct proc *, void *, register_t *);
int     sys_fchownat(struct proc *, void *, register_t *);
int     sys_linkat(struct proc *, void *, register_t *);
int     sys_mkdirat(struct proc *, void *, register_t *);
int     sys_mkfifoat(struct proc *, void *, register_t *);
int     sys_mknodat(struct proc *, void *, register_t *);
int     sys_openat(struct proc *, void *, register_t *);
int     sys_readlinkat(struct proc *, void *, register_t *);
int     sys_renameat(struct proc *, void *, register_t *);
int     sys_symlinkat(struct proc *, void *, register_t *);
int     sys_unlinkat(struct proc *, void *, register_t *);
int     sys___set_tcb(struct proc *, void *, register_t *);
int     sys___get_tcb(struct proc *, void *, register_t *);
int     sys_khello(struct proc *, void *, register_t *);
openbsd#
```



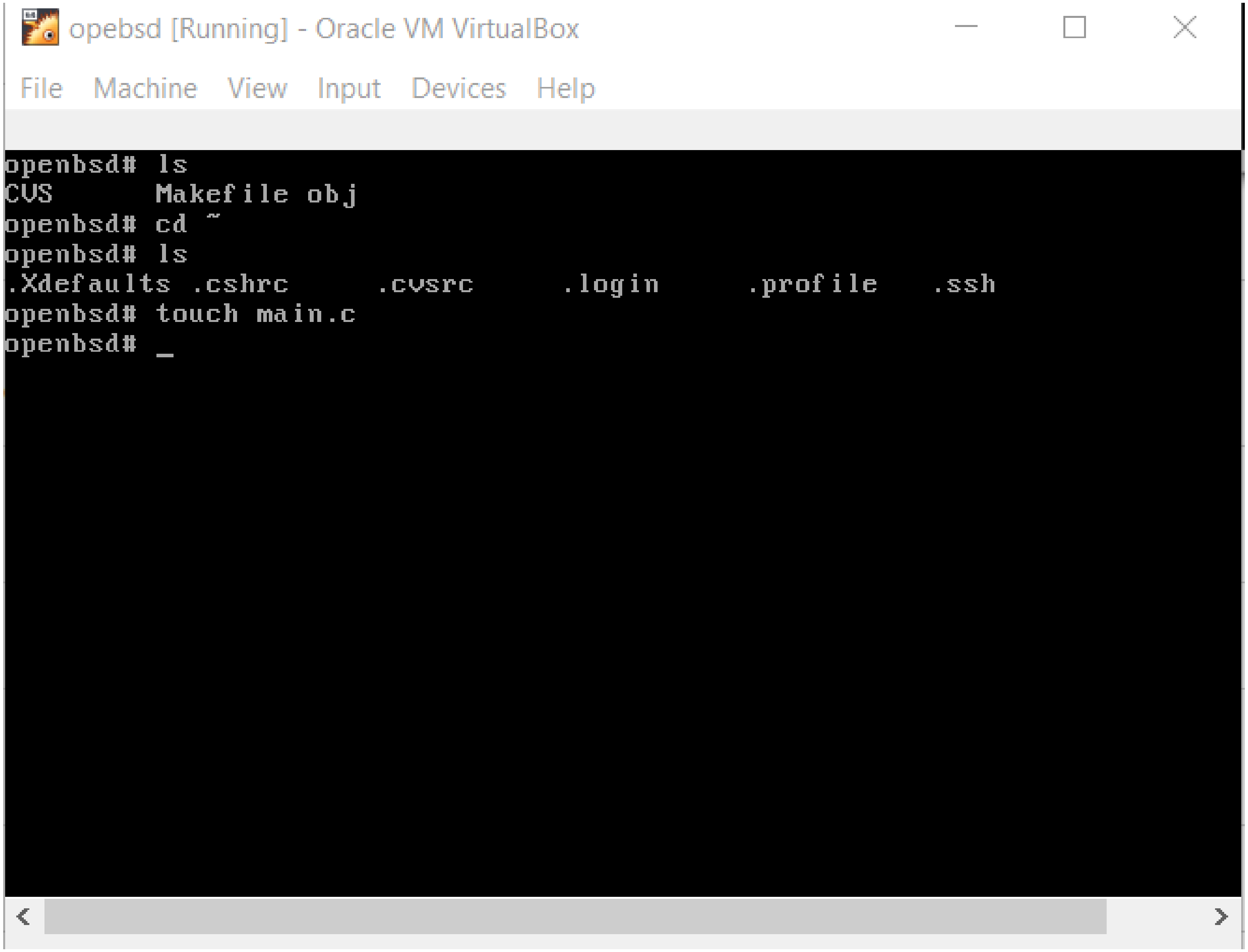
```
bad:
        if (pl != pfds)
                free(pl, M_TEMP, sz);
        return (error);
}

/*
 * utrace system call
 */
int
sys_utrace(struct proc *curp, void *v, register_t *retval)
{
#ifdef KTRACE
        struct sys_utrace_args /* {
                syscallarg(const char *) label;
                syscallarg(const void *) addr;
                syscallarg(size_t) len;
        } */ *uap = v;
        return (ktruser(curp, SCARG(uap, label), SCARG(uap, addr),
            SCARG(uap, len)));
#else
        return (0);
#endif
}
openbsd#
```



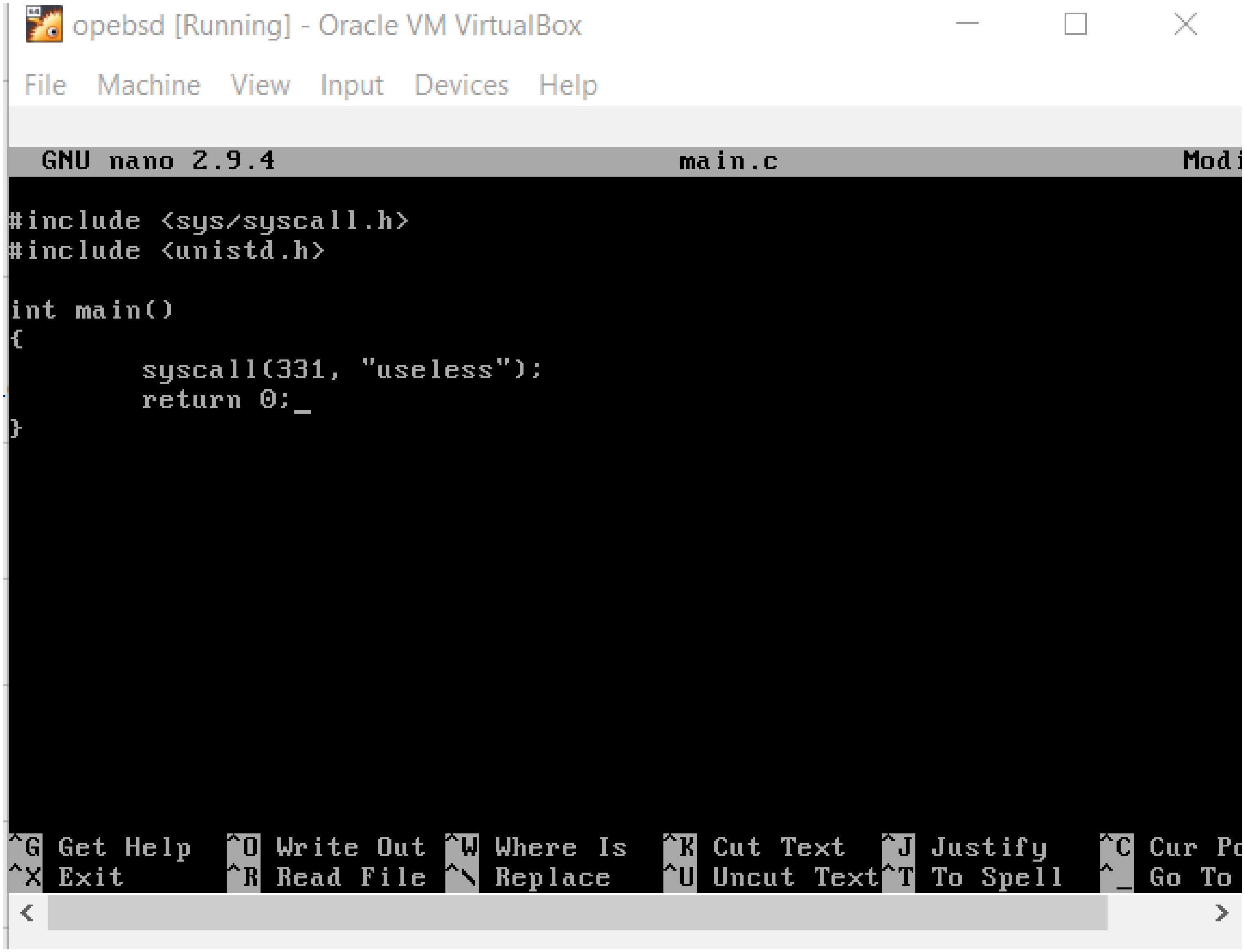
```
  GNU nano 2.9.4                    sys_generic.c                     Modified
                syscallarg(const char *) label;
                syscallarg(const void *) addr;
                syscallarg(size_t) len;
        } */ *uap = v;
        return (ktruser(curp, SCARG(uap, label), SCARG(uap, addr),
            SCARG(uap, len)));
#else
        return (0);
#endif
}


int
sys_khello(struct proc *p, void *v, register_t *retval)
{
        printf("Hello World!\n");
        return 0;
}




openbsd# _
```



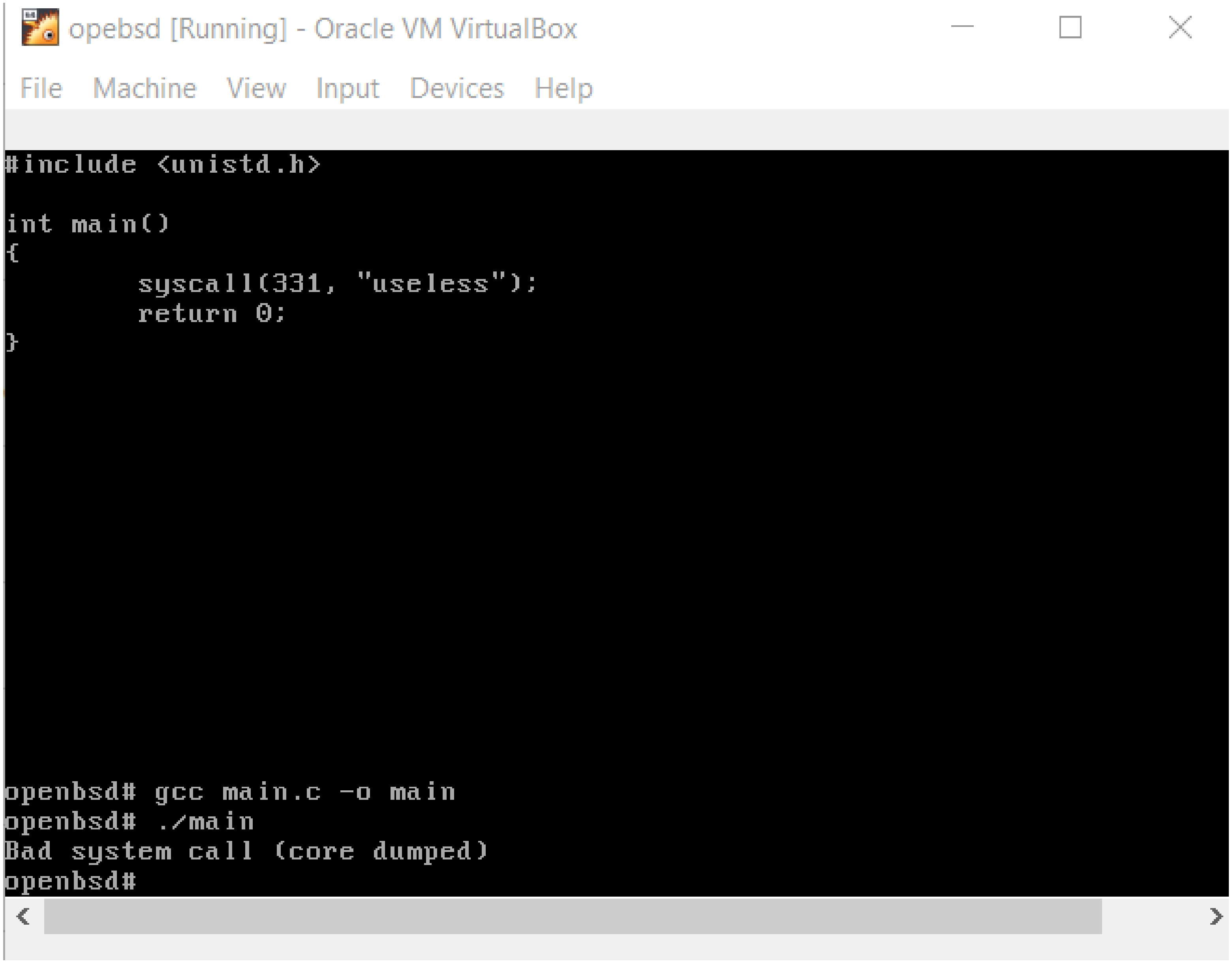
```
-DPIPEX -DMROUTING -DMPLS -DBOOT_CONFIG -DUSER_PCICONF -DAPERTURE -DMTRR -
-DHIBERNATE -DPCIVERBOSE -DUSBVERBOSE -DWSDISPLAY_COMPAT_USL -DWSDISPLAY_C
RAWKBD -DWSDISPLAY_DEFAULTSCREENS="6" -DX86EMU -DONEWIREVERBOSE -DMULTIPRO
 -DMAXUSERS=80 -D_KERNEL -MD -MP  -c ioconf.c
sh /sys/conf/newvers.sh
cc -g -Werror -Wall -Wimplicit-function-declaration  -Wno-uninitialized -W
nter-sign  -Wno-address-of-packed-member -Wno-constant-conversion  -Wframe
r-than=2047 -mcmodel=kernel -mno-red-zone -mno-sse2 -mno-sse -mno-3dnow  -
x -msoft-float -fno-omit-frame-pointer -ffreestanding -fno-pie -O2 -pipe -
nc -I/sys -I/sys/arch/amd64/compile/GENERIC.MP/obj -I/sys/arch -DDDB -DDIA
C -DKTRACE -DACCOUNTING -DKMEMSTATS -DPTRACE -DCRYPTO -DSYSVMSG -DSYSVSEM
SHM -DUVM_SWAP_ENCRYPT -DFFS -DFFS2 -DFFS_SOFTUPDATES -DUFS_DIRHASH -DQUOT
T2FS -DMFS -DNFSCLIENT -DNFSSERVER -DCD9660 -DUDF -DMSDOSFS -DFIFO -DFUSE
ET_SPLICE -DTCP_ECN -DTCP_SIGNATURE -DINET6 -DIPSEC -DPPP_BSDCOMP -DPPP_DE
-DPIPEX -DMROUTING -DMPLS -DBOOT_CONFIG -DUSER_PCICONF -DAPERTURE -DMTRR -
-DHIBERNATE -DPCIVERBOSE -DUSBVERBOSE -DWSDISPLAY_COMPAT_USL -DWSDISPLAY_C
RAWKBD -DWSDISPLAY_DEFAULTSCREENS="6" -DX86EMU -DONEWIREVERBOSE -DMULTIPRO
 -DMAXUSERS=80 -D_KERNEL -MD -MP  -c vers.c
LD="ld" sh makegap.sh 0xcccccccc
ld -T ld.script -X --warn-common -nopie -o bsd ${SYSTEM_HEAD} vers.o ${OBJ
text    data    bss     dec     hex
8618719 2708864 667648  11995231        b7085f
mv bsd bsd.gdb
ctfstrip -S -o bsd bsd.gdb
openbsd#
```



```
openbsd# ls
CVS      Makefile obj
openbsd# cd ~
openbsd# ls
.Xdefaults .cshrc     .cvsrc     .login     .profile   .ssh
openbsd# touch main.c
openbsd# _
```

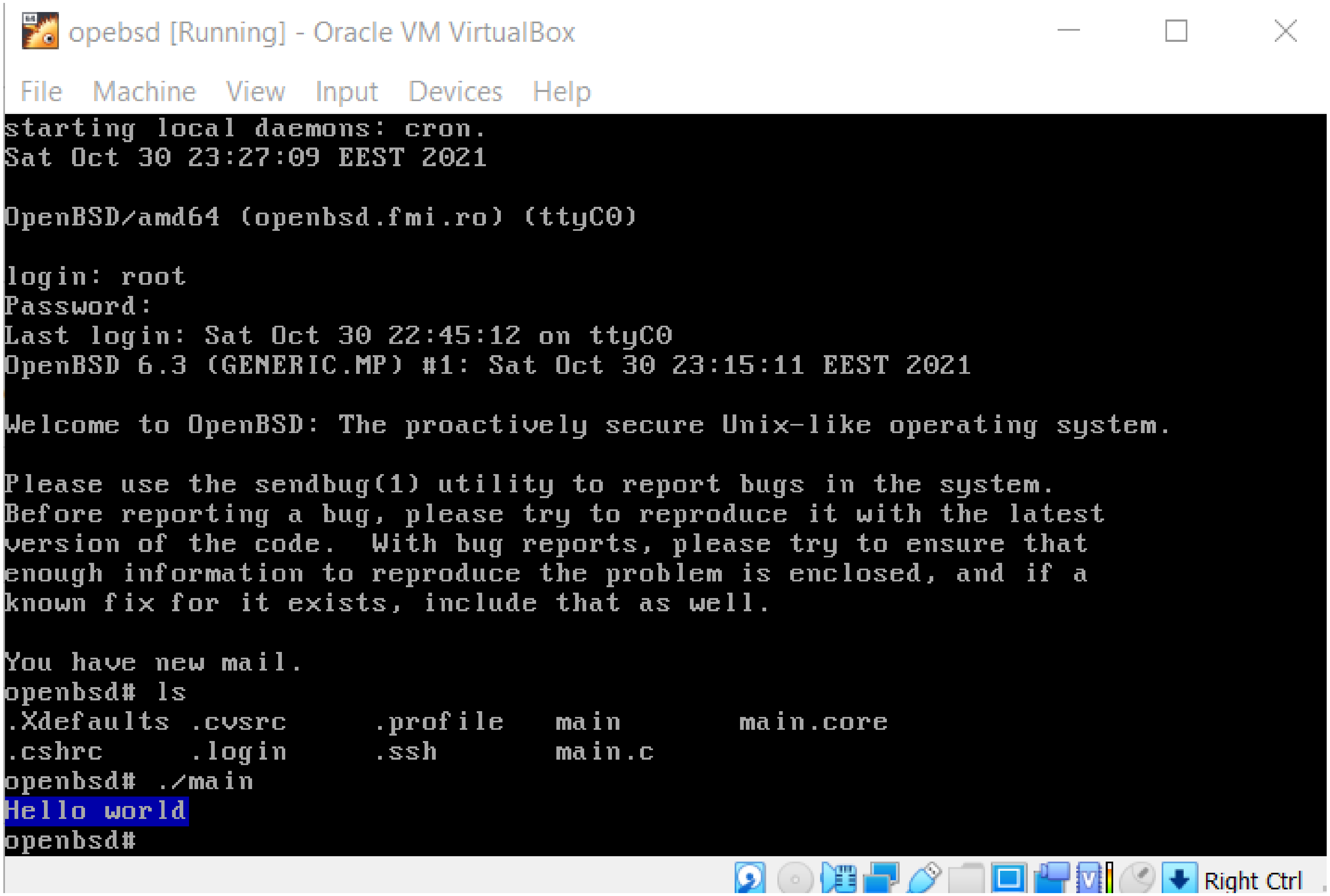


```
#include <sys/syscall.h>
#include <unistd.h>

int main()
{
        syscall(331, "useless");
        return 0;
}
```

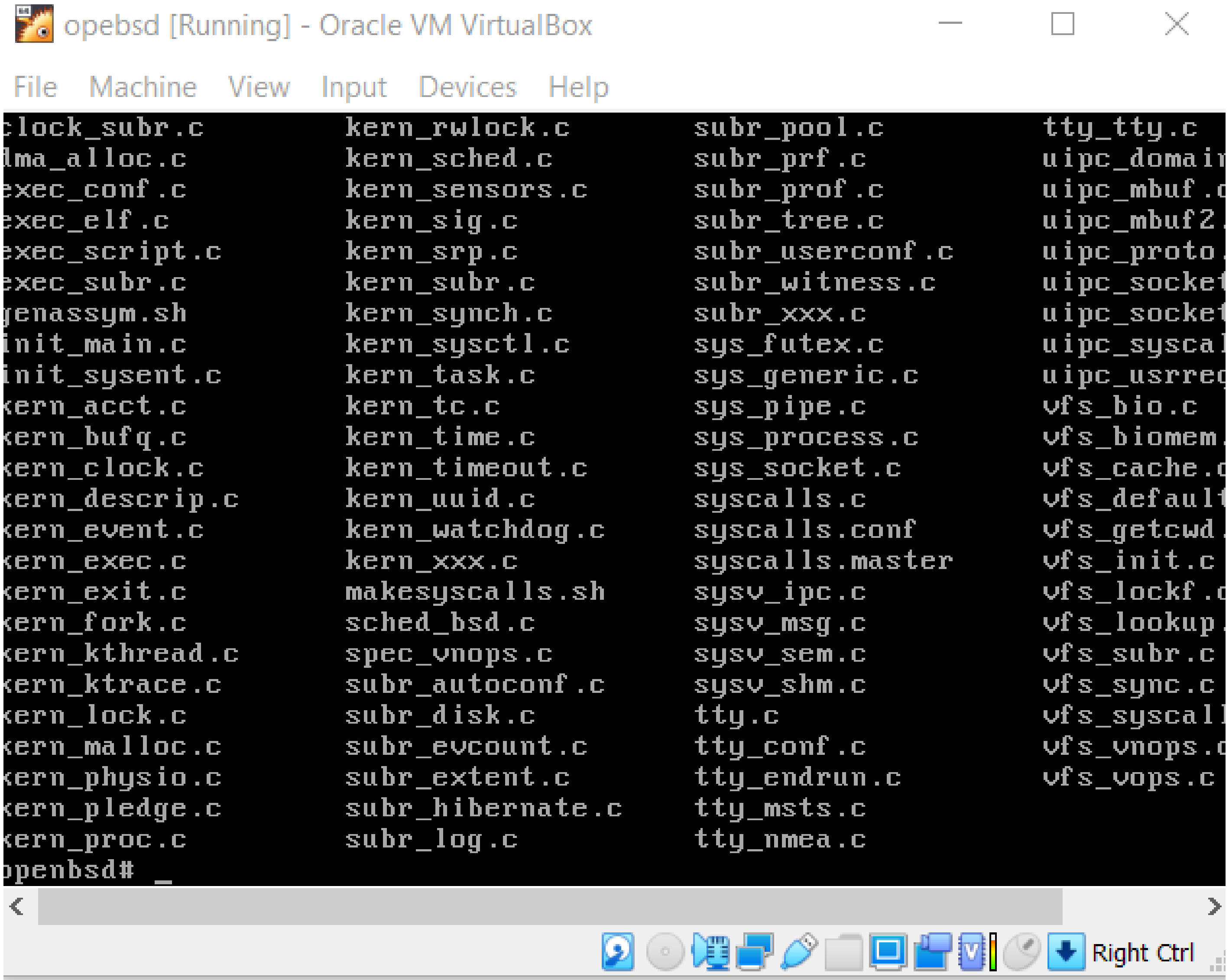


```
#include <unistd.h>

int main()
{
        syscall(331, "useless");
        return 0;
}
```

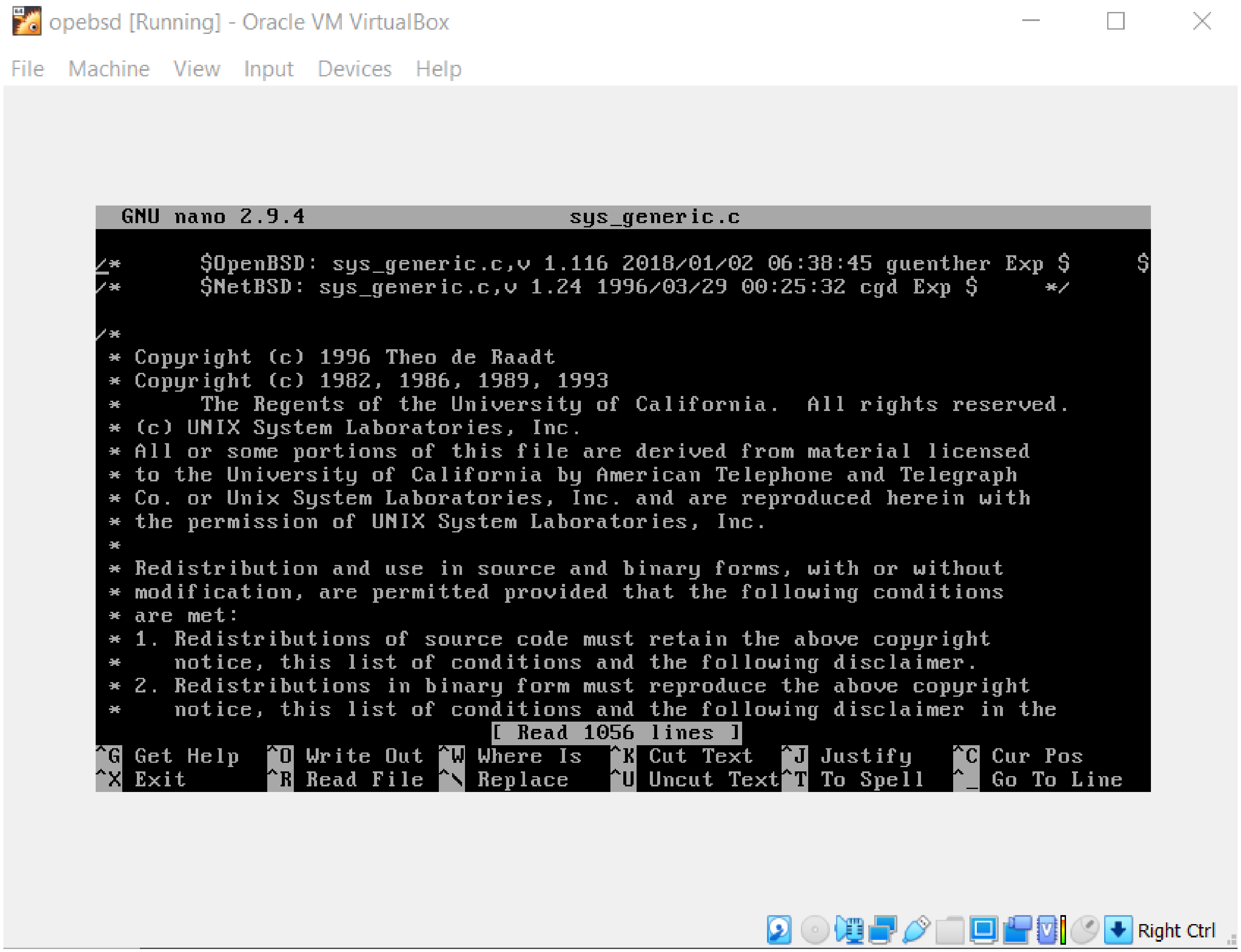
```
openbsd# gcc main.c -o main
openbsd# ./main
Bad system call (core dumped)
openbsd#
```


opebsd [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

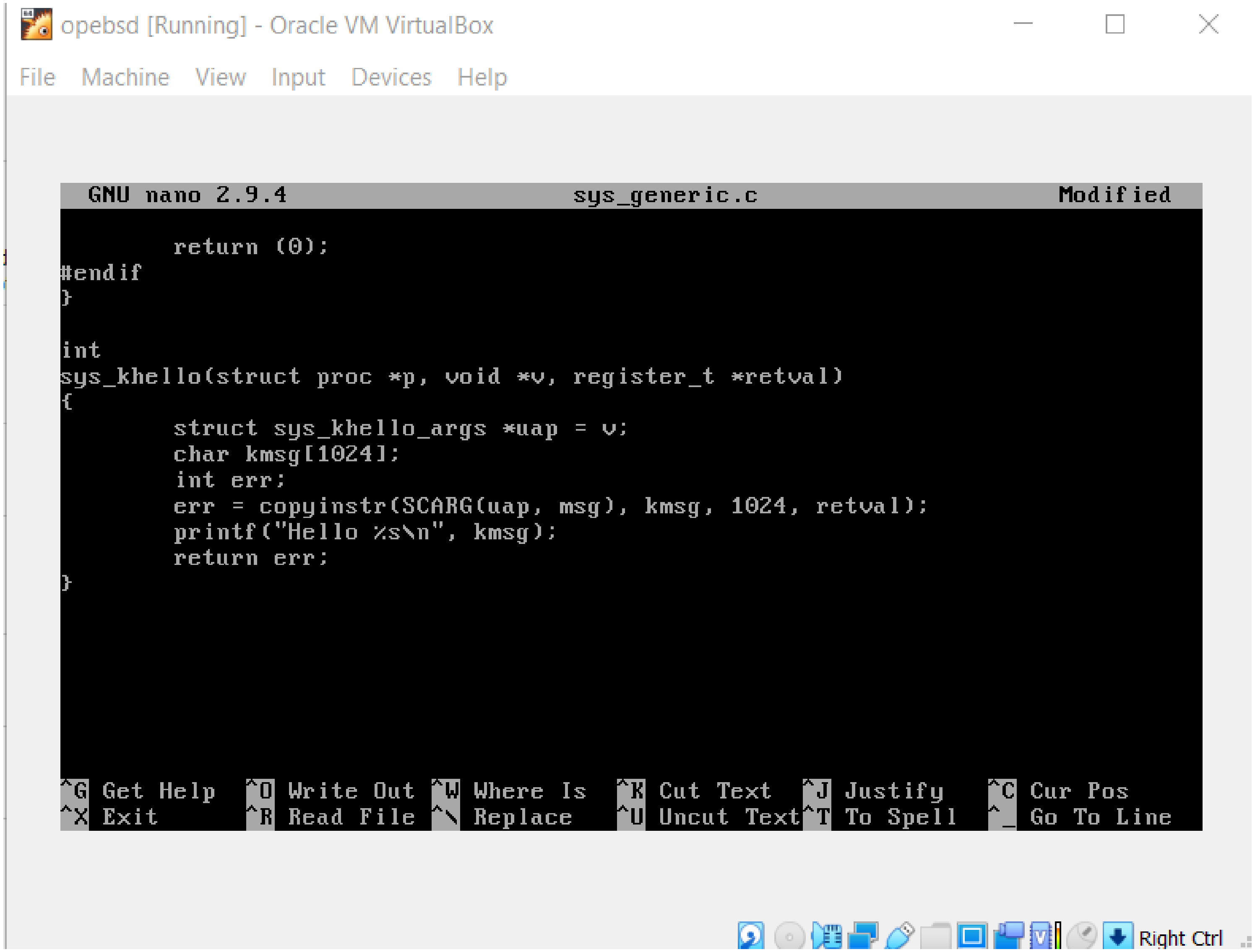
```
starting local daemons: cron.
Sat Oct 30 23:27:09 EEST 2021

OpenBSD/amd64 (openbsd.fmi.ro) (ttyC0)

login: root
Password:
Last login: Sat Oct 30 22:45:12 on ttyC0
OpenBSD 6.3 (GENERIC.MP) #1: Sat Oct 30 23:15:11 EEST 2021

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

You have new mail.
openbsd# ls
.Xdefaults .cvsrc      .profile    main        main.core
.cshrc     .login      .ssh        main.c
openbsd# ./main
Hello world
openbsd#
```



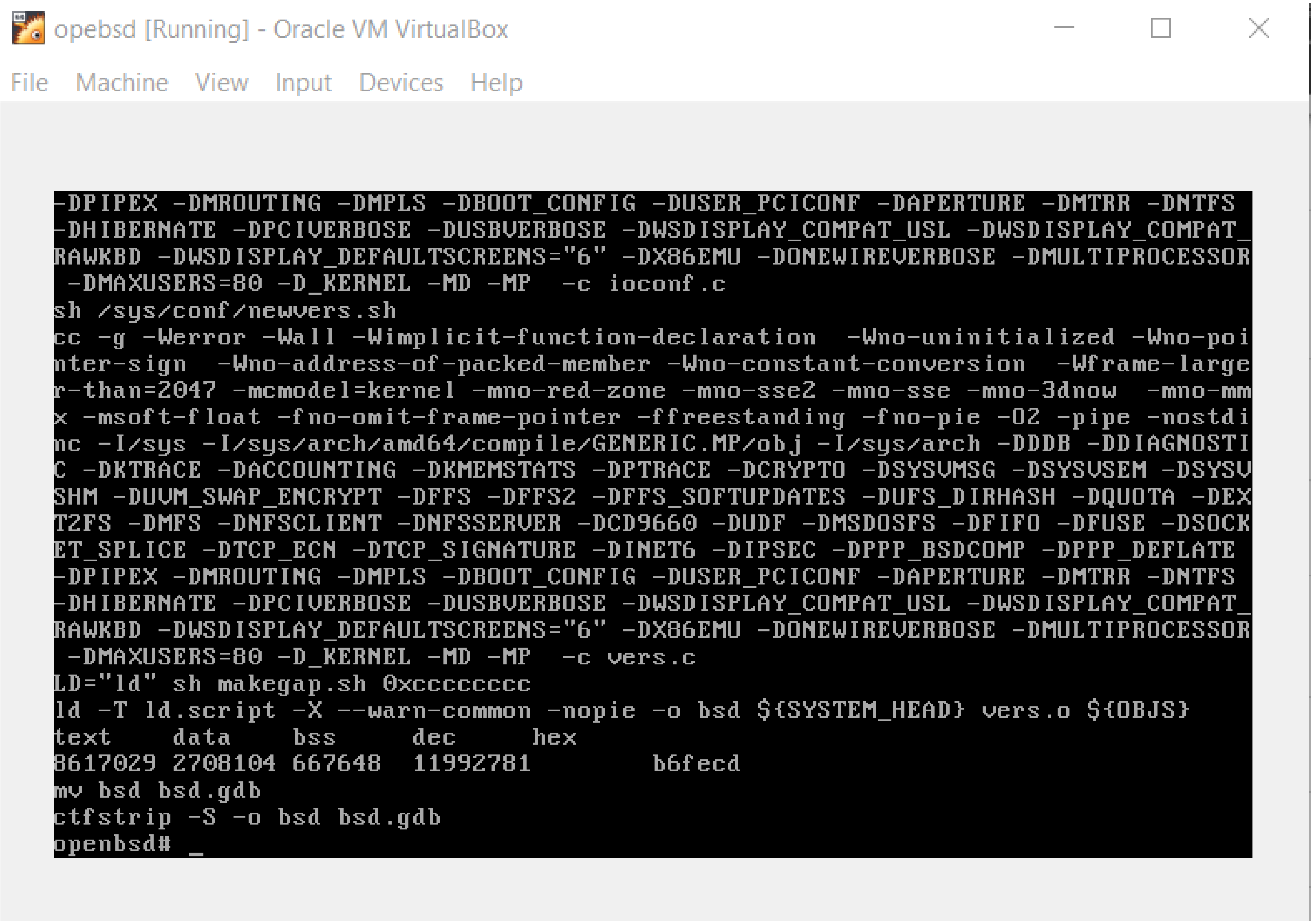
```
clock_subr.c        kern_rwlock.c       subr_pool.c         tty_tty.c
dma_alloc.c         kern_sched.c        subr_prf.c          uipc_domai
exec_conf.c         kern_sensors.c      subr_prof.c         uipc_mbuf.c
exec_elf.c          kern_sig.c          subr_tree.c         uipc_mbuf2.
exec_script.c       kern_srp.c          subr_userconf.c     uipc_proto.
exec_subr.c         kern_subr.c         subr_witness.c      uipc_socket
genassym.sh         kern_synch.c        subr_xxx.c          uipc_socket
init_main.c         kern_sysctl.c       sys_futex.c         uipc_syscal
init_sysent.c       kern_task.c         sys_generic.c       uipc_usrreq
kern_acct.c         kern_tc.c           sys_pipe.c          vfs_bio.c
kern_bufq.c         kern_time.c         sys_process.c       vfs_biomem.
kern_clock.c        kern_timeout.c      sys_socket.c        vfs_cache.c
kern_descrip.c      kern_uuid.c         syscalls.c          vfs_default
kern_event.c        kern_watchdog.c     syscalls.conf       vfs_getcwd.
kern_exec.c         kern_xxx.c          syscalls.master     vfs_init.c
kern_exit.c         makesyscalls.sh     sysv_ipc.c          vfs_lockf.c
kern_fork.c         sched_bsd.c         sysv_msg.c          vfs_lookup.
kern_kthread.c      spec_vnops.c        sysv_sem.c          vfs_subr.c
kern_ktrace.c       subr_autoconf.c     sysv_shm.c          vfs_sync.c
kern_lock.c         subr_disk.c         tty.c               vfs_syscall
kern_malloc.c       subr_evcount.c      tty_conf.c          vfs_vnops.c
kern_physio.c       subr_extent.c       tty_endrun.c        vfs_vops.c
kern_pledge.c       subr_hibernate.c    tty_msts.c
kern_proc.c         subr_log.c          tty_nmea.c
openbsd# _
```



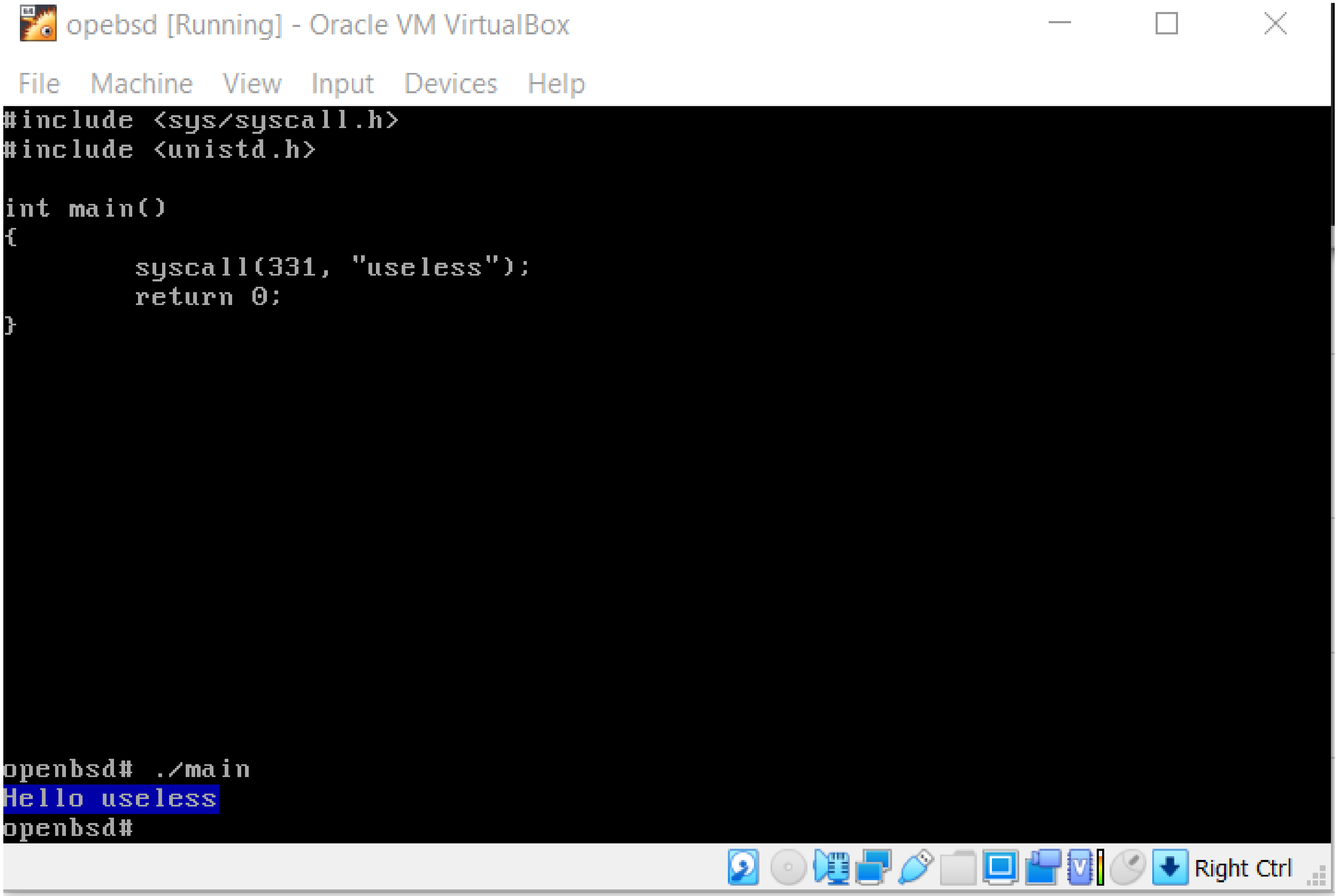
```
 GNU nano 2.9.4                        sys_generic.c

/*      $OpenBSD: sys_generic.c,v 1.116 2018/01/02 06:38:45 guenther Exp $     $
/*      $NetBSD: sys_generic.c,v 1.24 1996/03/29 00:25:32 cgd Exp $      */

/*
 * Copyright (c) 1996 Theo de Raadt
 * Copyright (c) 1982, 1986, 1989, 1993
 *      The Regents of the University of California.  All rights reserved.
 * (c) UNIX System Laboratories, Inc.
 * All or some portions of this file are derived from material licensed
 * to the University of California by American Telephone and Telegraph
 * Co. or Unix System Laboratories, Inc. and are reproduced herein with
 * the permission of UNIX System Laboratories, Inc.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
                            [ Read 1056 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```


opebsd [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
  GNU nano 2.9.4                    sys_generic.c                      Modified

        return (0);
#endif
}

int
sys_khello(struct proc *p, void *v, register_t *retval)
{
        struct sys_khello_args *uap = v;
        char kmsg[1024];
        int err;
        err = copyinstr(SCARG(uap, msg), kmsg, 1024, retval);
        printf("Hello %s\n", kmsg);
        return err;
}

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```

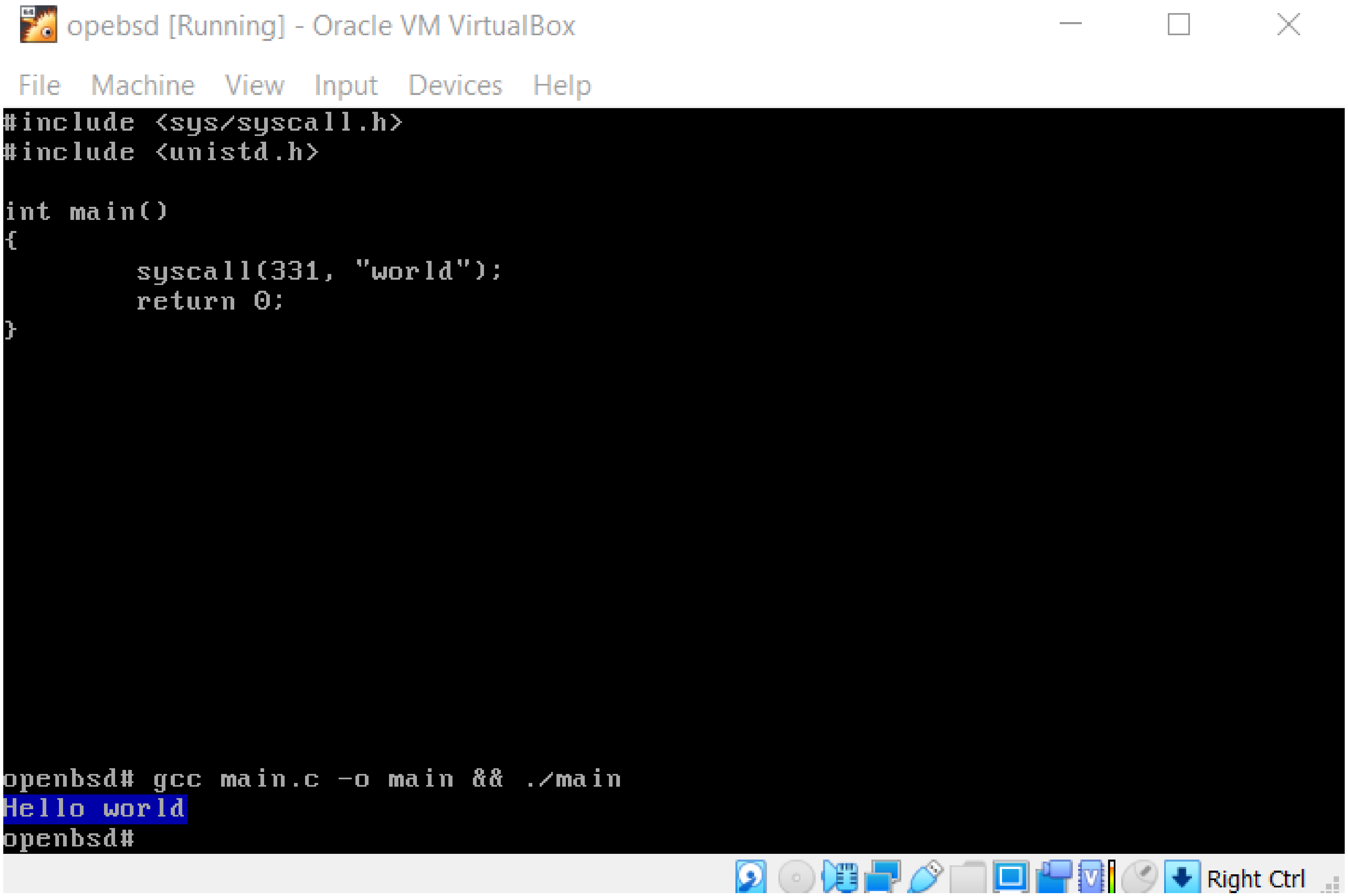


```
-DPIPEX -DMROUTING -DMPLS -DBOOT_CONFIG -DUSER_PCICONF -DAPERTURE -DMTRR -DNTFS
-DHIBERNATE -DPCIVERBOSE -DUSBVERBOSE -DWSDISPLAY_COMPAT_USL -DWSDISPLAY_COMPAT_
RAWKBD -DWSDISPLAY_DEFAULTSCREENS="6" -DX86EMU -DONEWIREVERBOSE -DMULTIPROCESSOR
 -DMAXUSERS=80 -D_KERNEL -MD -MP  -c ioconf.c
sh /sys/conf/newvers.sh
cc -g -Werror -Wall -Wimplicit-function-declaration  -Wno-uninitialized -Wno-poi
nter-sign  -Wno-address-of-packed-member -Wno-constant-conversion  -Wframe-large
r-than=2047 -mcmodel=kernel -mno-red-zone -mno-sse2 -mno-sse -mno-3dnow  -mno-mm
x -msoft-float -fno-omit-frame-pointer -ffreestanding -fno-pie -O2 -pipe -nostdi
nc -I/sys -I/sys/arch/amd64/compile/GENERIC.MP/obj -I/sys/arch -DDDB -DDIAGNOSTI
C -DKTRACE -DACCOUNTING -DKMEMSTATS -DPTRACE -DCRYPTO -DSYSVMSG -DSYSVSEM -DSYSV
SHM -DUVM_SWAP_ENCRYPT -DFFS -DFFS2 -DFFS_SOFTUPDATES -DUFS_DIRHASH -DQUOTA -DEX
T2FS -DMFS -DNFSCLIENT -DNFSSERVER -DCD9660 -DUDF -DMSDOSFS -DFIFO -DFUSE -DSOCK
ET_SPLICE -DTCP_ECN -DTCP_SIGNATURE -DINET6 -DIPSEC -DPPP_BSDCOMP -DPPP_DEFLATE
-DPIPEX -DMROUTING -DMPLS -DBOOT_CONFIG -DUSER_PCICONF -DAPERTURE -DMTRR -DNTFS
-DHIBERNATE -DPCIVERBOSE -DUSBVERBOSE -DWSDISPLAY_COMPAT_USL -DWSDISPLAY_COMPAT_
RAWKBD -DWSDISPLAY_DEFAULTSCREENS="6" -DX86EMU -DONEWIREVERBOSE -DMULTIPROCESSOR
 -DMAXUSERS=80 -D_KERNEL -MD -MP  -c vers.c
LD="ld" sh makegap.sh 0xcccccccc
ld -T ld.script -X --warn-common -nopie -o bsd ${SYSTEM_HEAD} vers.o ${OBJS}
text    data    bss     dec     hex
8617029 2708104 667648  11992781        b6fecd
mv bsd bsd.gdb
ctfstrip -S -o bsd bsd.gdb
openbsd# _
```



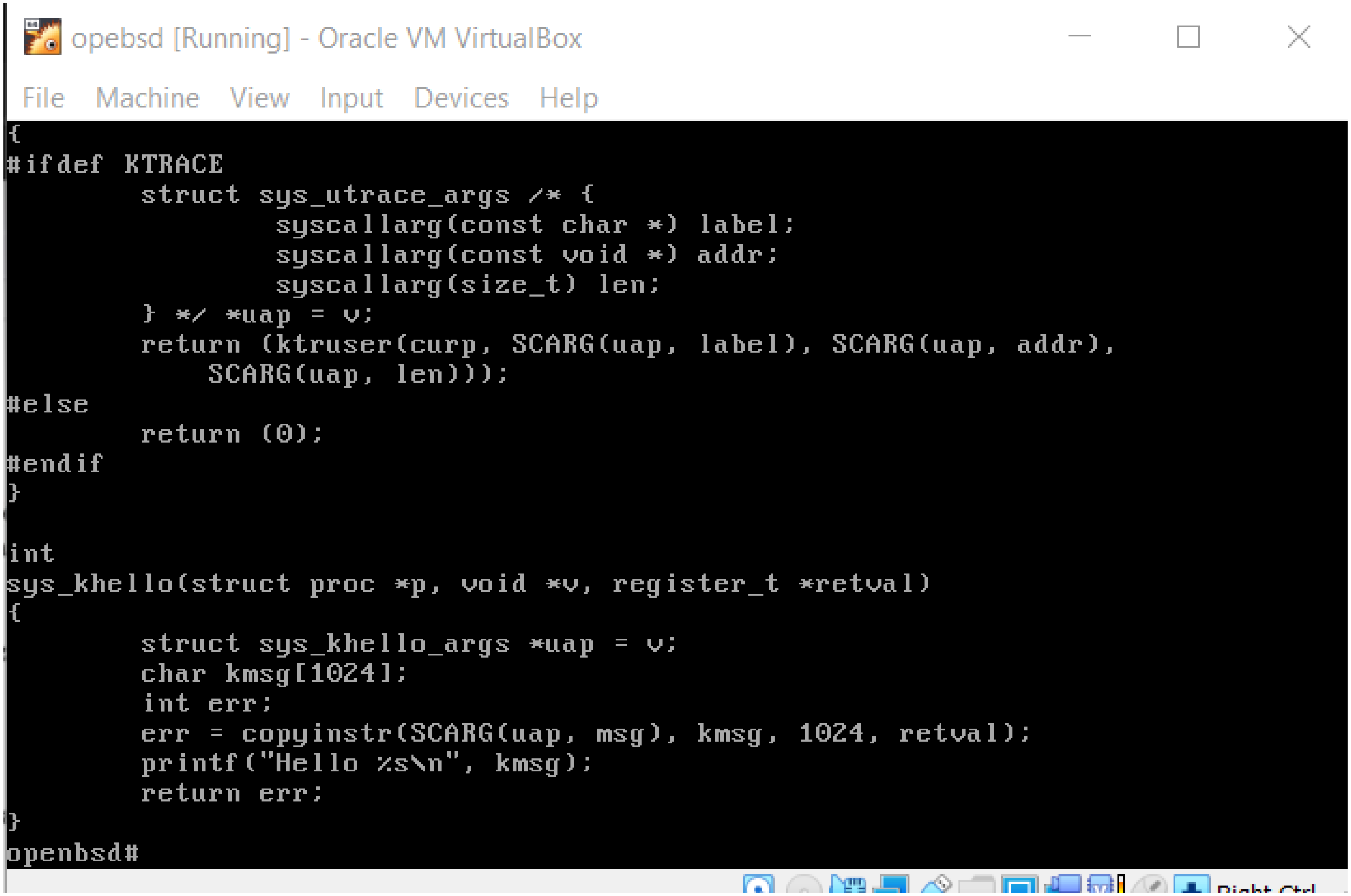
```
#include <sys/syscall.h>
#include <unistd.h>

int main()
{
        syscall(331, "useless");
        return 0;
}
```

```
openbsd# ./main
Hello useless
openbsd#
```



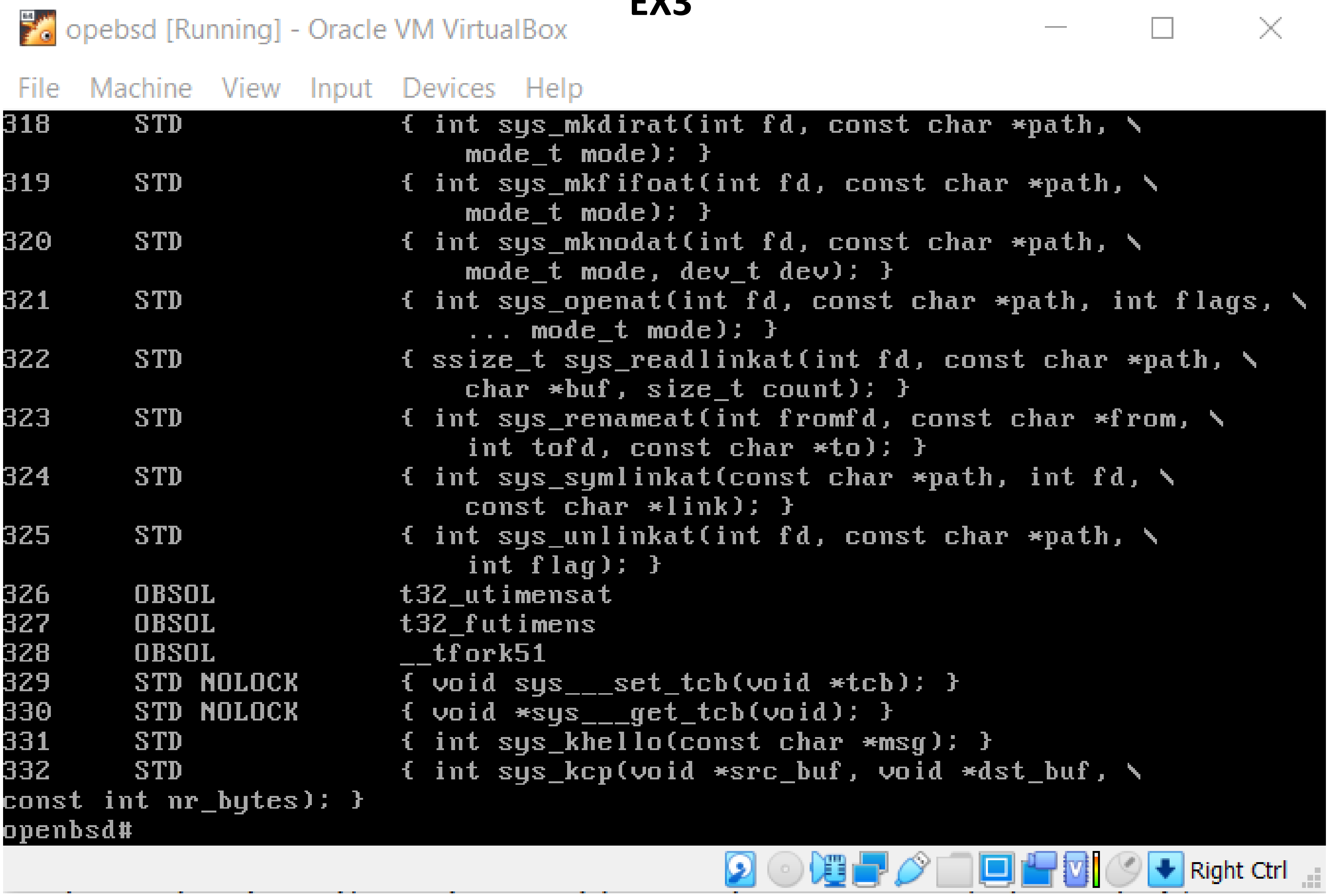
```
#include <sys/syscall.h>
#include <unistd.h>

int main()
{
        syscall(331, "world");
        return 0;
}
```

```
openbsd# gcc main.c -o main && ./main
Hello world
openbsd#
```

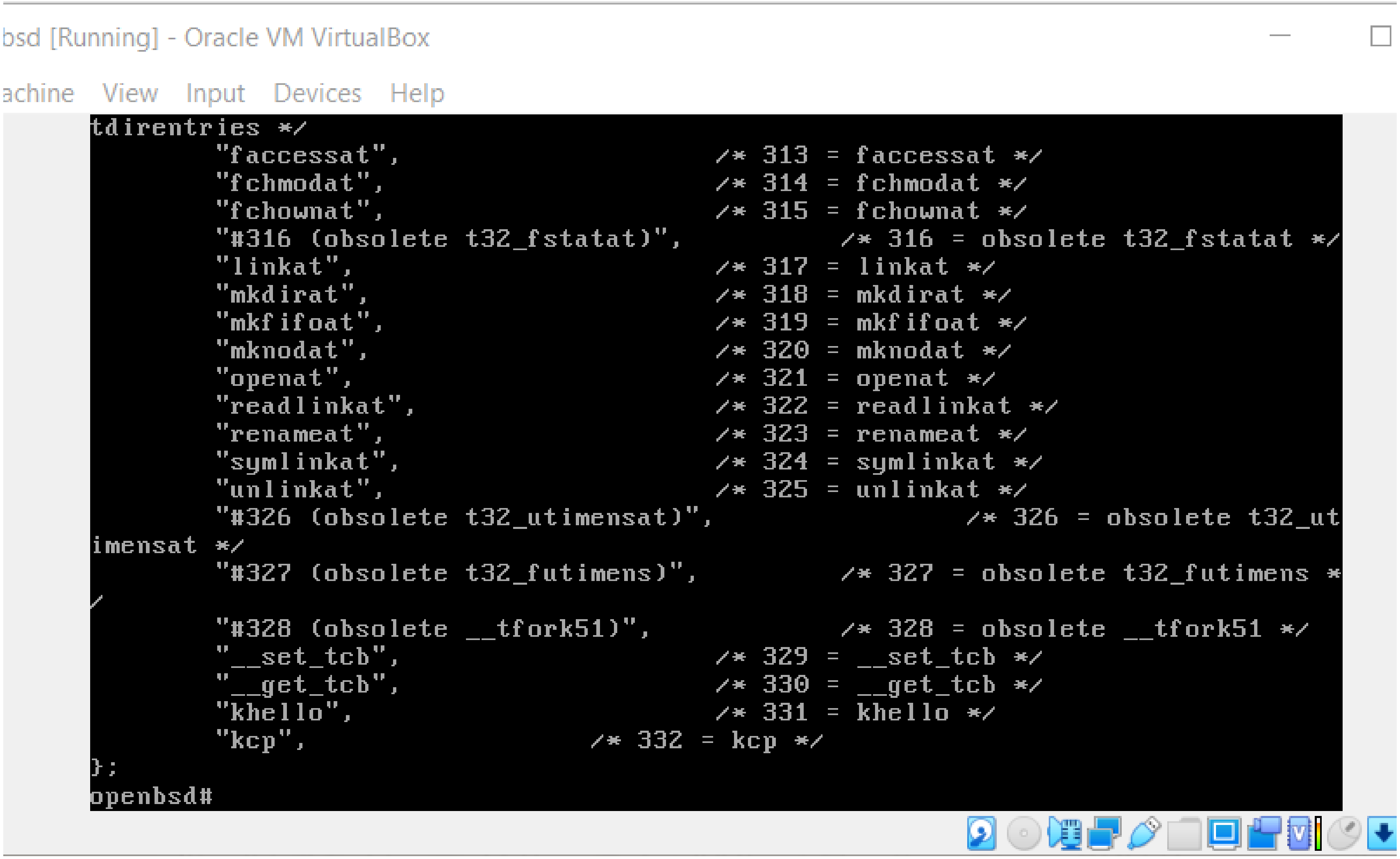


```
{
#ifdef KTRACE
        struct sys_utrace_args /* {
                syscallarg(const char *) label;
                syscallarg(const void *) addr;
                syscallarg(size_t) len;
        } */ *uap = v;
        return (ktruser(curp, SCARG(uap, label), SCARG(uap, addr),
            SCARG(uap, len)));
#else
        return (0);
#endif
}

int
sys_khello(struct proc *p, void *v, register_t *retval)
{
        struct sys_khello_args *uap = v;
        char kmsg[1024];
        int err;
        err = copyinstr(SCARG(uap, msg), kmsg, 1024, retval);
        printf("Hello %s\n", kmsg);
        return err;
}
openbsd#
```

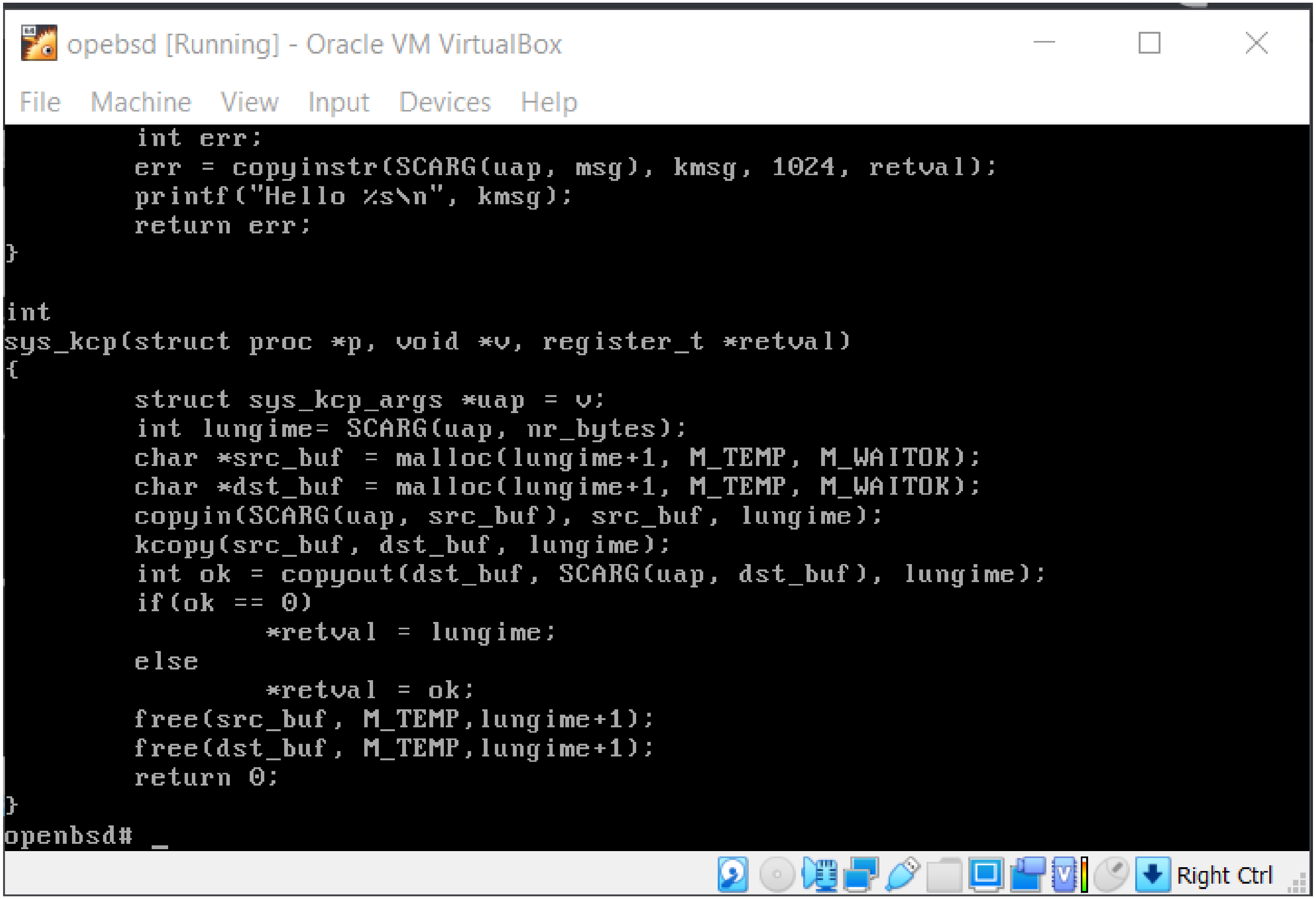
EX3



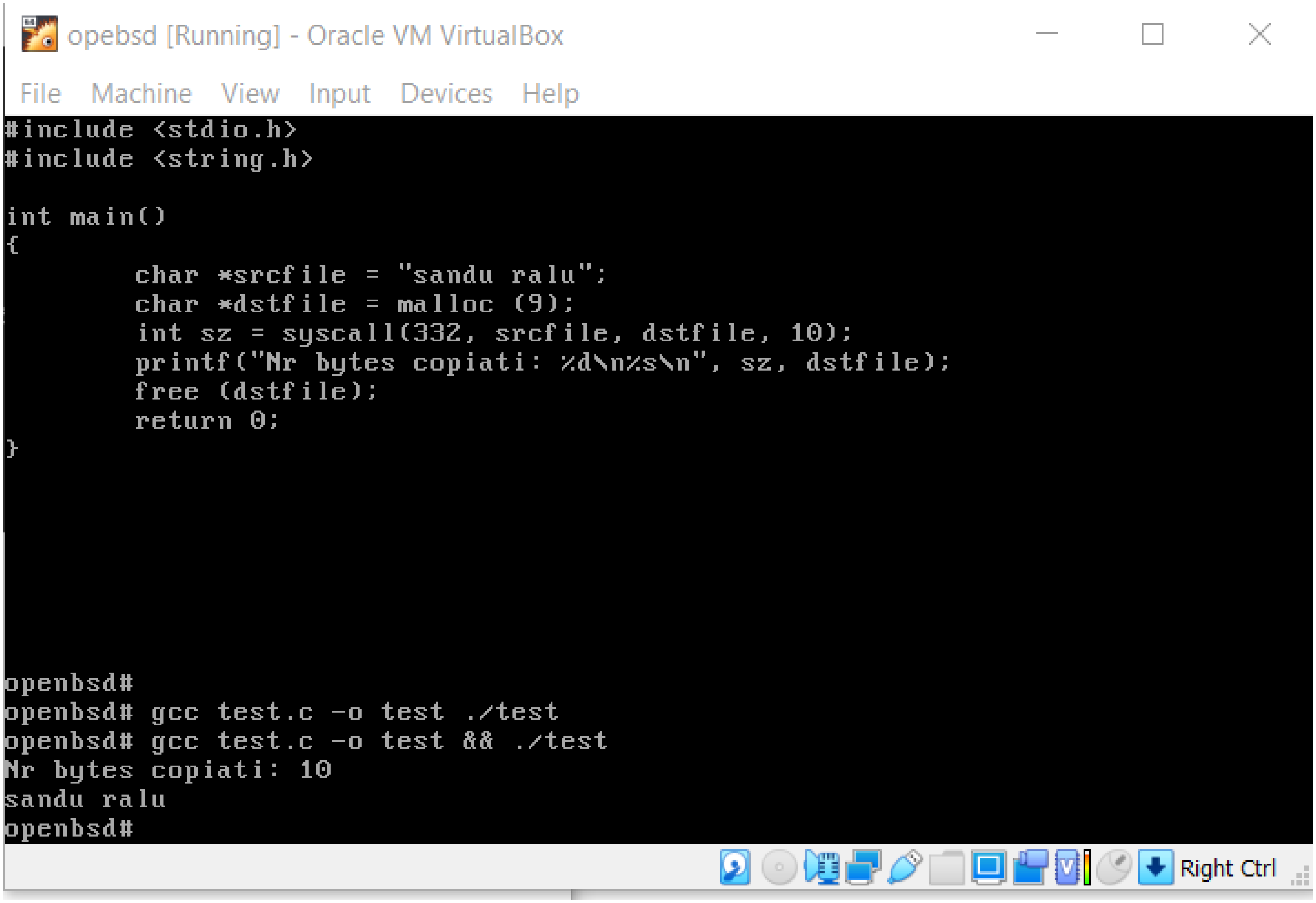
```
318     STD                     { int sys_mkdirat(int fd, const char *path, \
                                    mode_t mode); }
319     STD                     { int sys_mkfifoat(int fd, const char *path, \
                                    mode_t mode); }
320     STD                     { int sys_mknodat(int fd, const char *path, \
                                    mode_t mode, dev_t dev); }
321     STD                     { int sys_openat(int fd, const char *path, int flags, \
                                    ... mode_t mode); }
322     STD                     { ssize_t sys_readlinkat(int fd, const char *path, \
                                    char *buf, size_t count); }
323     STD                     { int sys_renameat(int fromfd, const char *from, \
                                    int tofd, const char *to); }
324     STD                     { int sys_symlinkat(const char *path, int fd, \
                                    const char *link); }
325     STD                     { int sys_unlinkat(int fd, const char *path, \
                                    int flag); }
326     OBSOL                   t32_utimensat
327     OBSOL                   t32_futimens
328     OBSOL                   __tfork51
329     STD NOLOCK              { void sys___set_tcb(void *tcb); }
330     STD NOLOCK              { void *sys___get_tcb(void); }
331     STD                     { int sys_khello(const char *msg); }
332     STD                     { int sys_kcp(void *src_buf, void *dst_buf, \
const int nr_bytes); }
openbsd#
```



```
tdirentries */
        "faccessat",                    /* 313 = faccessat */
        "fchmodat",                     /* 314 = fchmodat */
        "fchownat",                     /* 315 = fchownat */
        "#316 (obsolete t32_fstatat)",          /* 316 = obsolete t32_fstatat */
        "linkat",                       /* 317 = linkat */
        "mkdirat",                      /* 318 = mkdirat */
        "mkfifoat",                     /* 319 = mkfifoat */
        "mknodat",                      /* 320 = mknodat */
        "openat",                       /* 321 = openat */
        "readlinkat",                   /* 322 = readlinkat */
        "renameat",                     /* 323 = renameat */
        "symlinkat",                    /* 324 = symlinkat */
        "unlinkat",                     /* 325 = unlinkat */
        "#326 (obsolete t32_utimensat)",                /* 326 = obsolete t32_ut
imensat */
        "#327 (obsolete t32_futimens)",         /* 327 = obsolete t32_futimens *
/
        "#328 (obsolete __tfork51)",            /* 328 = obsolete __tfork51 */
        "__set_tcb",                    /* 329 = __set_tcb */
        "__get_tcb",                    /* 330 = __get_tcb */
        "khello",                       /* 331 = khello */
        "kcp",                  /* 332 = kcp */
};
openbsd#
```



```
        int err;
        err = copyinstr(SCARG(uap, msg), kmsg, 1024, retval);
        printf("Hello %s\n", kmsg);
        return err;
}

int
sys_kcp(struct proc *p, void *v, register_t *retval)
{
        struct sys_kcp_args *uap = v;
        int lungime= SCARG(uap, nr_bytes);
        char *src_buf = malloc(lungime+1, M_TEMP, M_WAITOK);
        char *dst_buf = malloc(lungime+1, M_TEMP, M_WAITOK);
        copyin(SCARG(uap, src_buf), src_buf, lungime);
        kcopy(src_buf, dst_buf, lungime);
        int ok = copyout(dst_buf, SCARG(uap, dst_buf), lungime);
        if(ok == 0)
                *retval = lungime;
        else
                *retval = ok;
        free(src_buf, M_TEMP,lungime+1);
        free(dst_buf, M_TEMP,lungime+1);
        return 0;
}
openbsd# _
```



```
#include <stdio.h>
#include <string.h>

int main()
{
        char *srcfile = "sandu ralu";
        char *dstfile = malloc (9);
        int sz = syscall(332, srcfile, dstfile, 10);
        printf("Nr bytes copiati: %d\n%s\n", sz, dstfile);
        free (dstfile);
        return 0;
}
```

```
openbsd#
openbsd# gcc test.c -o test ./test
openbsd# gcc test.c -o test && ./test
Nr bytes copiati: 10
sandu ralu
openbsd#
```