File manager window showing bigbangtheory-master folder with files: learnord_win.exe, README.md, sheldon1, sheldon2. Right-click context menu with options: New Folder (Shift+Ctrl+N), Paste (Ctrl+V), Select All (Ctrl+A), Properties, Open in Terminal.

Terminal window:

```
root@kali: ~/Downloads/bigbangtheory-master
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads/bigbangtheory-master# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
```

```
root@kali:~/Downloads/bigbangtheory-master# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!




ls


BOOM!!!
The bomb has blown up.
root@kali:~/Downloads/bigbangtheory-master#
```

```
root@kali:~/Downloads/bigbangtheory-master# gdb sheldon1
GNU gdb (Debian 8.1-4+b1) 8.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from sheldon1...done.
(gdb) disass sheldon1
No symbol "sheldon1" in current context.
(gdb) set disassembly -flavor intel
Undefined item: "-flavor intel".
(gdb) disassemble main
Dump of assembler code for function main:
```

File   Edit   View   Search   Terminal   Help

```
   0x08048a0b <+91>:      call    0x8048850 <exit@plt>
   0x08048a10 <+96>:      add     $0xfffffff8,%esp
   0x08048a13 <+99>:      mov     (%ebx),%eax
   0x08048a15 <+101>:     push    %eax
   0x08048a16 <+102>:     push    $0x804963f
   0x08048a1b <+107>:     call    0x8048810 <printf@plt>
   0x08048a20 <+112>:     add     $0xfffffff4,%esp
   0x08048a23 <+115>:     push    $0x8
   0x08048a25 <+117>:     call    0x8048850 <exit@plt>
   0x08048a2a <+122>:     lea     0x0(%esi),%esi
   0x08048a30 <+128>:     call    0x8049160 <initialize_bomb>
   0x08048a35 <+133>:     add     $0xfffffff4,%esp
   0x08048a38 <+136>:     push    $0x8049660
---Type <return> to continue, or q <return> to quit---r
   0x08048a3d <+141>:     call    0x8048810 <printf@plt>
   0x08048a42 <+146>:     add     $0xfffffff4,%esp
   0x08048a45 <+149>:     push    $0x80496a0
   0x08048a4a <+154>:     call    0x8048810 <printf@plt>
   0x08048a4f <+159>:     add     $0x20,%esp
   0x08048a52 <+162>:     call    0x80491fc <read_line>
   0x08048a57 <+167>:     add     $0xfffffff4,%esp
   0x08048a5a <+170>:     push    %eax
   0x08048a5b <+171>:     call    0x8048b20 <phase_1>
   0x08048a60 <+176>:     call    0x804952c <phase_defused>
```

Home   Downloads   bigbangthe

Recent

learnord_
win.exe

READM
md

Starred

Home

Documents

Music

Pictures

```
   0x08048aab <+251>:     add      $0xfffffff4,%esp
   0x08048aae <+254>:     push     $0x804973f
   0x08048ab3 <+259>:     call     0x8048810 <printf@plt>
   0x08048ab8 <+264>:     add      $0x20,%esp
   0x08048abb <+267>:     call     0x80491fc <read_line>
   0x08048ac0 <+272>:     add      $0xfffffff4,%esp
   0x08048ac3 <+275>:     push     %eax
   0x08048ac4 <+276>:     call     0x8048ce0 <phase_4>
   0x08048ac9 <+281>:     call     0x804952c <phase_defused>
   0x08048ace <+286>:     add      $0xfffffff4,%esp
   0x08048ad1 <+289>:     push     $0x8049760
   0x08048ad6 <+294>:     call     0x8048810 <printf@plt>
   0x08048adb <+299>:     add      $0x20,%esp
   0x08048ade <+302>:     call     0x80491fc <read_line>
   0x08048ae3 <+307>:     add      $0xfffffff4,%esp
   0x08048ae6 <+310>:     push     %eax
   0x08048ae7 <+311>:     call     0x8048d2c <phase_5>
   0x08048aec <+316>:     call     0x804952c <phase_defused>
---Type <return> to continue, or q <return> to quit---r
   0x08048af1 <+321>:     add      $0xfffffff4,%esp
   0x08048af4 <+324>:     push     $0x80497a0
   0x08048af9 <+329>:     call     0x8048810 <printf@plt>
   0x08048afe <+334>:     add      $0x20,%esp
   0x08048b01 <+337>:     call     0x80491fc <read_line>
   0x08048b06 <+342>:     add      $0xfffffff4,%esp
   0x08048b09 <+345>:     push     %eax
   0x08048b0a <+346>:     call     0x8048d98 <phase_6>
   0x08048b0f <+351>:     call     0x804952c <phase_defused>
   0x08048b14 <+356>:     xor      %eax,%eax
   0x08048b16 <+358>:     mov      -0x18(%ebp),%ebx
   0x08048b19 <+361>:     mov      %ebp,%esp
   0x08048b1b <+363>:     pop      %ebp
   0x08048b1c <+364>:     ret
End of assembler dump.
(gdb) x 0x804952c
0x804952c <phase_defused>:       0x83e58955
(gdb) break * 0x83e58955
Breakpoint 1 at 0x83e58955
(gdb)
```

```
End of assembler dump.
(gdb) x 0x804952c
0x804952c <phase_defused>:        0x83e58955
(gdb) break * 0x83e58955
Breakpoint 1 at 0x83e58955
(gdb) x/32xw $esp
No registers.
(gdb) run AAAAA
Starting program: /root/Downloads/bigbangtheory-master/sheldon1 AAAAA
Warning:
Cannot insert breakpoint 1.
Cannot access memory at address 0x83e58955

(gdb) x/32xw $esp
0xffffd300:        0x00000002        0xffffd492        0xffffd4c0        0x00000000
0xffffd310:        0xffffd4c6        0xffffdaa8        0xffffdabf        0xffffdace
0xffffd320:        0xffffdadf        0xffffdaf4        0xffffdb03        0xffffdb0e
0xffffd330:        0xffffdb3d        0xffffdb51        0xffffdb5f        0xffffdb6a
0xffffd340:        0xffffdb90        0xffffdba1        0xffffdbab        0xffffdbc1
0xffffd350:        0xffffdc17        0xffffdc40        0xffffdc49        0xffffdc54
0xffffd360:        0xffffdc6b        0xffffdc7d        0xffffdc90        0xffffdca5
0xffffd370:        0xffffdce2        0xffffdcfc        0xffffdd51        0xffffdd6d
(gdb) run AAAAA
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /root/Downloads/bigbangtheory-master/sheldon1 AAAAA
Warning:
Cannot insert breakpoint 1.
Cannot access memory at address 0x83e58955
```

```
root@kali:~/Downloads/bigbangtheory-master# gdb sheldon1
GNU gdb (Debian 8.1-4+b1) 8.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from sheldon1...done.
(gdb) break phase_1
Breakpoint 1 at 0x8048b26
(gdb) run
Starting program: /root/Downloads/bigbangtheory-master/sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!

test string

Breakpoint 1, 0x08048b26 in phase_1 ()
(gdb) p/x $eax
$1 = 0x804b680
(gdb) x/25c 0x804b680
0x804b680 <input_strings>:     116 't' 101 'e' 115 's' 116 't' 32 ' '  115 's' 116 't' 114 'r'
0x804b688 <input_strings+8>:   105 'i' 110 'n' 103 'g' 0 '\000'     0 '\000'     0 '\000'     0 '\000'     0 '\000'
0x804b690 <input_strings+16>:  0 '\000'      0 '\000'     0 '\000'     0 '\000'     0 '\000'     0 '\000'     0 '\000'     0 '\000'
0x804b698 <input_strings+24>:  0 '\000'
(gdb) x/25c 0x80497c0
0x80497c0:      80 'P' 117 'u' 98 'b'  108 'l' 105 'i' 99 'c'  32 ' '  115 's'
0x80497c8:      112 'p' 101 'e' 97 'a'  107 'k' 105 'i' 110 'n' 103 'g' 32 ' '
0x80497d0:      105 'i' 115 's' 32 ' '  118 'v' 101 'e' 114 'r' 121 'y' 32 ' '
0x80497d8:      101 'e'
(gdb)
```

```
nobo
%s: Error: Couldn't open %s
Usage: %s [<input_file>]
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Phase 1 defused. How about the next one?
That's number 2.  Keep going!
Halfway there!
So you got that one.  Try this one.
Good work!  On to the next...
Public speaking is very easy.
%d %c %d
giants
Wow! You've defused the secret stage!
whitefish.cmcl.cs.cmu.edu
warmouth.cmcl.cs.cmu.edu
walleye.cmcl.cs.cmu.edu
sturgeon.cmcl.cs.cmu.edu
striper.cmcl.cs.cmu.edu
sockeye.cmcl.cs.cmu.edu
sheepshead.cmcl.cs.cmu.edu
shad.cmcl.cs.cmu.edu
sauger.cmcl.cs.cmu.edu
salmon.cmcl.cs.cmu.edu
pumpkinseed.cmcl.cs.cmu.edu
pike.cmcl.cs.cmu.edu
pickerel.cmcl.cs.cmu.edu
perch.cmcl.cs.cmu.edu
paddlefish.cmcl.cs.cmu.edu
muskie.cmcl.cs.cmu.edu
minnow.cmcl.cs.cmu.edu
inconnu.cmcl.cs.cmu.edu
grayling.cmcl.cs.cmu.edu
gobi.cmcl.cs.cmu.edu
flier.cmcl.cs.cmu.edu
chum.cmcl.cs.cmu.edu
char.cmcl.cs.cmu.edu
bluegill.cmcl.cs.cmu.edu
bass.cmcl.cs.cmu.edu
So you think you can stop the bomb with ctrl-c, do you?
Well...
```

```
root@kali:~/Downloads/bigbangtheory-master# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Public speaking is very easy.
Phase 1 defused. How about the next one?
```

```
root@kali:~/Downloads/bigbangtheory-master# ./sheldon2
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

  _ /   _ /        _ /   _ /        _ /   _ /
 /_ /  /_ /       /_ /  /_ /       /_ /  /_ /
    HOURS            MINUTES          SECONDS
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
|                                                                   |
|         ,      DR. VON NOIZEMAN'S NUCLEAR BOMB   Downloads |
|       /!\ AUTHORIZED ACCESS ONLY - KEEP OUT /!\                    |
|                                                  ♫ Music          |
|       [1] YELLOW [2] GREEN [3] BLUE [4] RED                        |
|                                                     Pictures      |
|                                                                   |
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +

  MENU SELECTION: ls                               Videos
  PRESS ENTER TO RETURN TO MENU
KABOOM
                                                   Trash

            . ^^ - - - . . . , , - -
         _ - - /                    \ - - _          +  Other Locations
       < _                            > )
       |                               |
       \ . _                        _ . /
          - - . ` ` `      . - - ' ' '
              - - .  .  ,  ;  . - - '
                 |  |     |
              . -=| |   |  |=- .
              ` -=#$%&%$#=- '
                 |  ;   : |
       _____ . , -#%&$@%#&#~ , . _____
Segmentation fault
root@kali:~/Downloads/bigbangtheory-master# ls
```
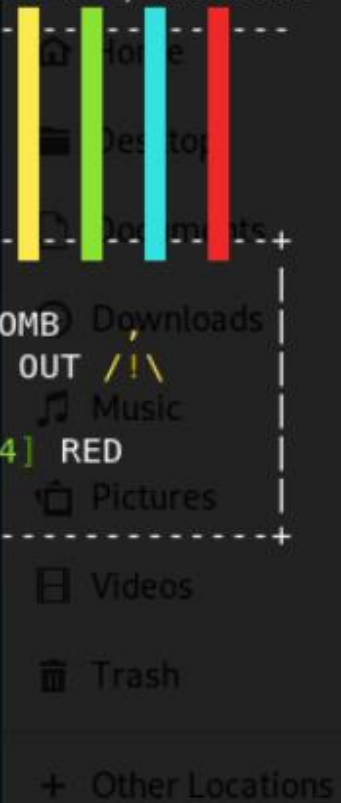
```
           ., -#%&$@%#&#~, .
Segmentation fault
root@kali:~/Downloads/bigbangtheory-master# ls
learnord_win.exe  README.md  sheldon1  sheldon2
root@kali:~/Downloads/bigbangtheory-master# gdb sheldon2
GNU gdb (Debian 8.1-4+b1) 8.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from sheldon2...done.
(gdb)
```