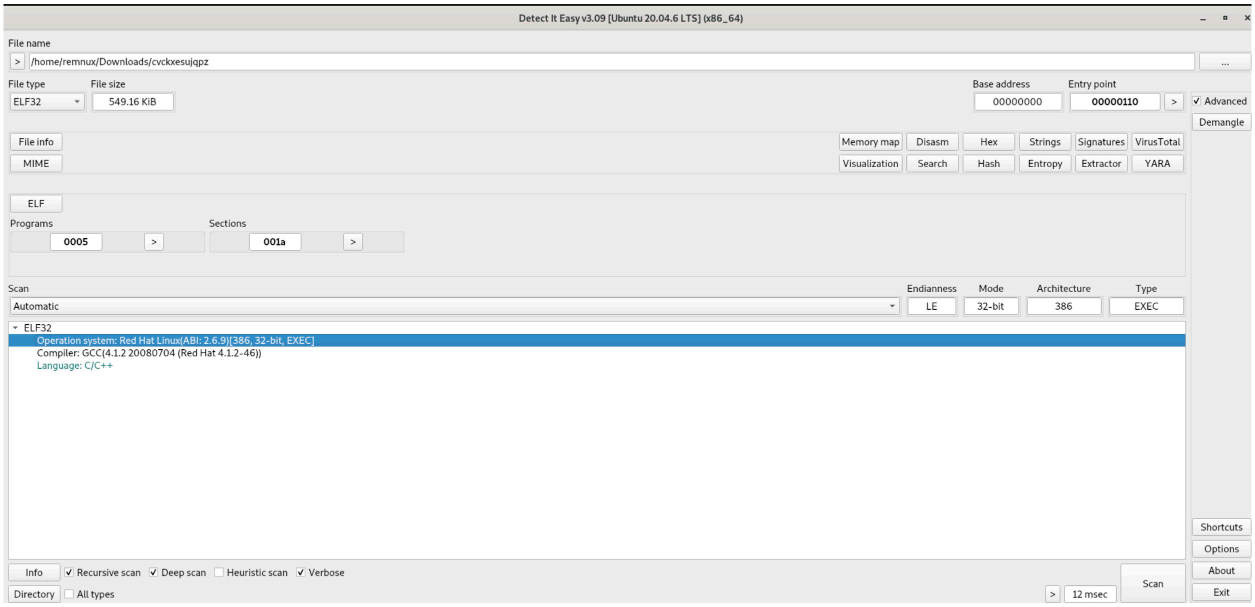


File name: /home/remnux/Downloads/cvckxesujqpz

File type: ELF32 File size: 549.16 KiB

Base address: 00000000 Entry point: 00000110 ☑ Advanced

Programs: 0005 Sections: 001a

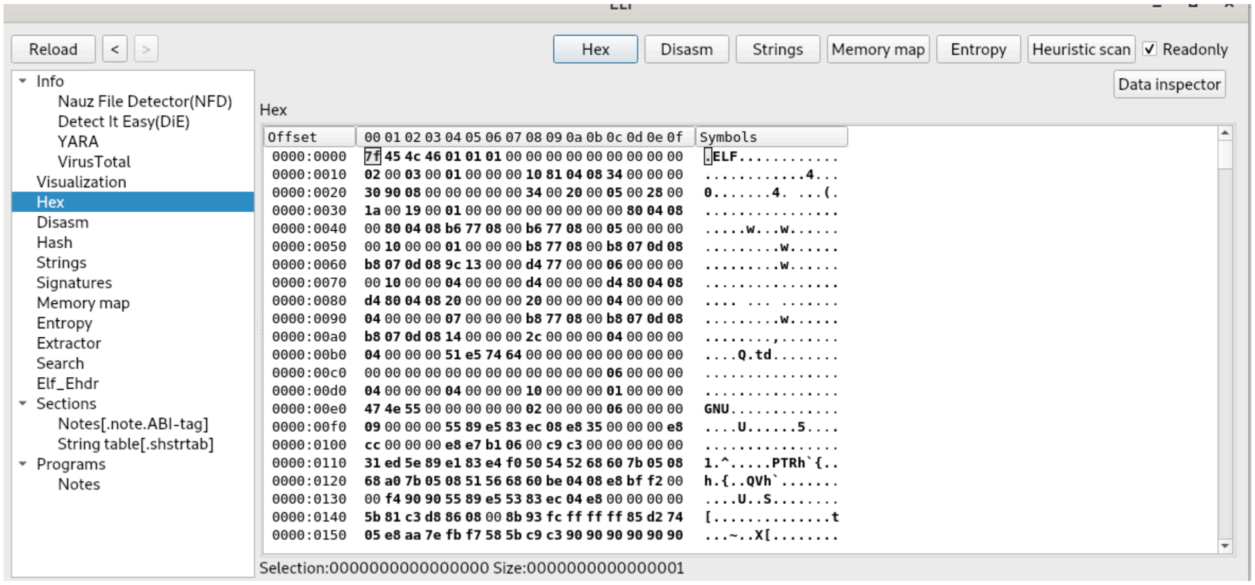
Scan: Automatic

Endianness: LE Mode: 32-bit Architecture: 386 Type: EXEC

```
ELF32
    Operation system: Red Hat Linux(ABI: 2.6.9)[386, 32-bit, EXEC]
    Compiler: GCC(4.1.2 20080704 (Red Hat 4.1.2-46))
    Language: C/C++
```

☑ Recursive scan ☑ Deep scan ☐ Heuristic scan ☑ Verbose ☐ All types

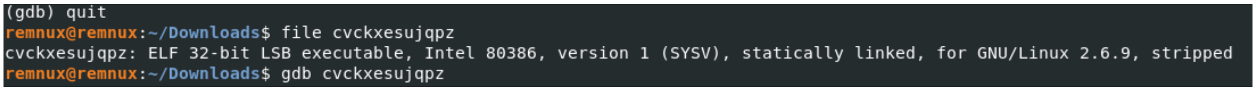
12 msec



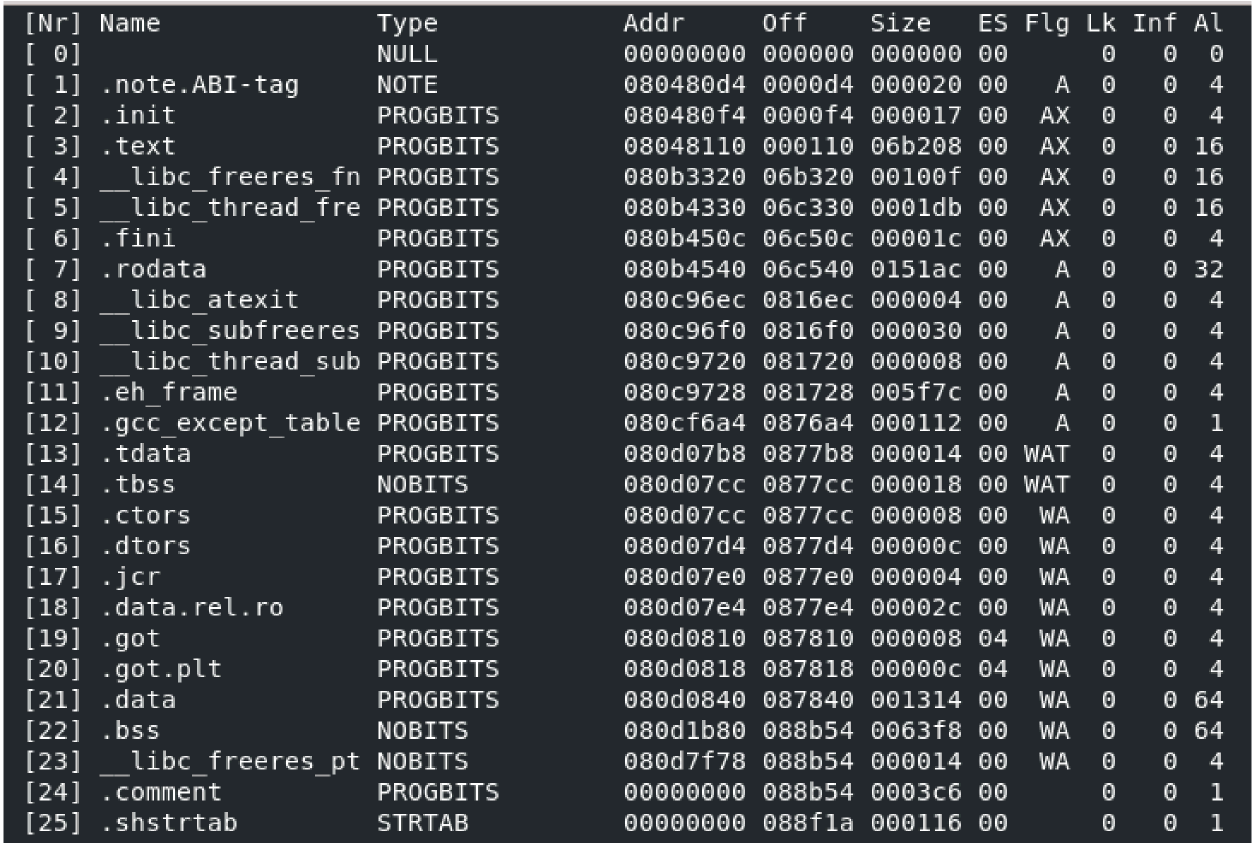
Hex

```
Offset      00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f   Symbols
 0000:0000  7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00   .ELF............
 0000:0010  02 00 03 00 01 00 00 00 10 81 04 08 34 00 00 00   ............4...
 0000:0020  30 90 08 00 00 00 00 00 34 00 20 00 05 00 28 00   0.......4. ...(.
 0000:0030  1a 00 19 00 01 00 00 00 00 00 00 00 00 80 04 08   ................
 0000:0040  00 80 04 08 b6 77 08 00 b6 77 08 00 05 00 00 00   .....w...w......
 0000:0050  00 10 00 00 01 00 00 00 b8 77 08 00 b8 07 0d 08   .........w......
 0000:0060  b8 07 0d 08 9c 13 00 00 d4 77 00 00 06 00 00 00   .........w......
 0000:0070  00 10 00 00 04 00 00 00 d4 00 00 00 d4 80 04 08   ................
 0000:0080  d4 80 04 08 20 00 00 00 20 00 00 00 04 00 00 00   ....  ...  .......
 0000:0090  04 00 00 00 07 00 00 00 b8 77 08 00 b8 07 0d 08   .........w......
 0000:00a0  b8 07 0d 08 14 00 00 00 2c 00 00 00 04 00 00 00   ........,.......
 0000:00b0  04 00 00 00 51 e5 74 64 00 00 00 00 00 00 00 00   ....Q.td........
 0000:00c0  00 00 00 00 00 00 00 00 00 00 00 00 06 00 00 00   ................
 0000:00d0  04 00 00 00 04 00 00 00 10 00 00 00 01 00 00 00   ................
 0000:00e0  47 4e 55 00 00 00 00 00 02 00 00 00 06 00 00 00   GNU.............
 0000:00f0  09 00 00 00 55 89 e5 83 ec 08 e8 35 00 00 00 e8   ....U......5....
 0000:0100  cc 00 00 00 e8 e7 b1 06 00 c9 c3 00 00 00 00 00   ................
 0000:0110  31 ed 5e 89 e1 83 e4 f0 50 54 52 68 60 7b 05 08   1.^.....PTRh`{..
 0000:0120  68 a0 7b 05 08 51 56 68 60 be 04 08 e8 bf f2 00   h.{..QVh`.......
 0000:0130  00 f4 90 90 55 89 e5 53 83 ec 04 e8 00 00 00 00   ....U..S........
 0000:0140  5b 81 c3 d8 86 08 00 8b 93 fc ff ff ff 85 d2 74   [..............t
 0000:0150  05 e8 aa 7e fb f7 58 5b c9 c3 90 90 90 90 90 90   ...~..X[........
```

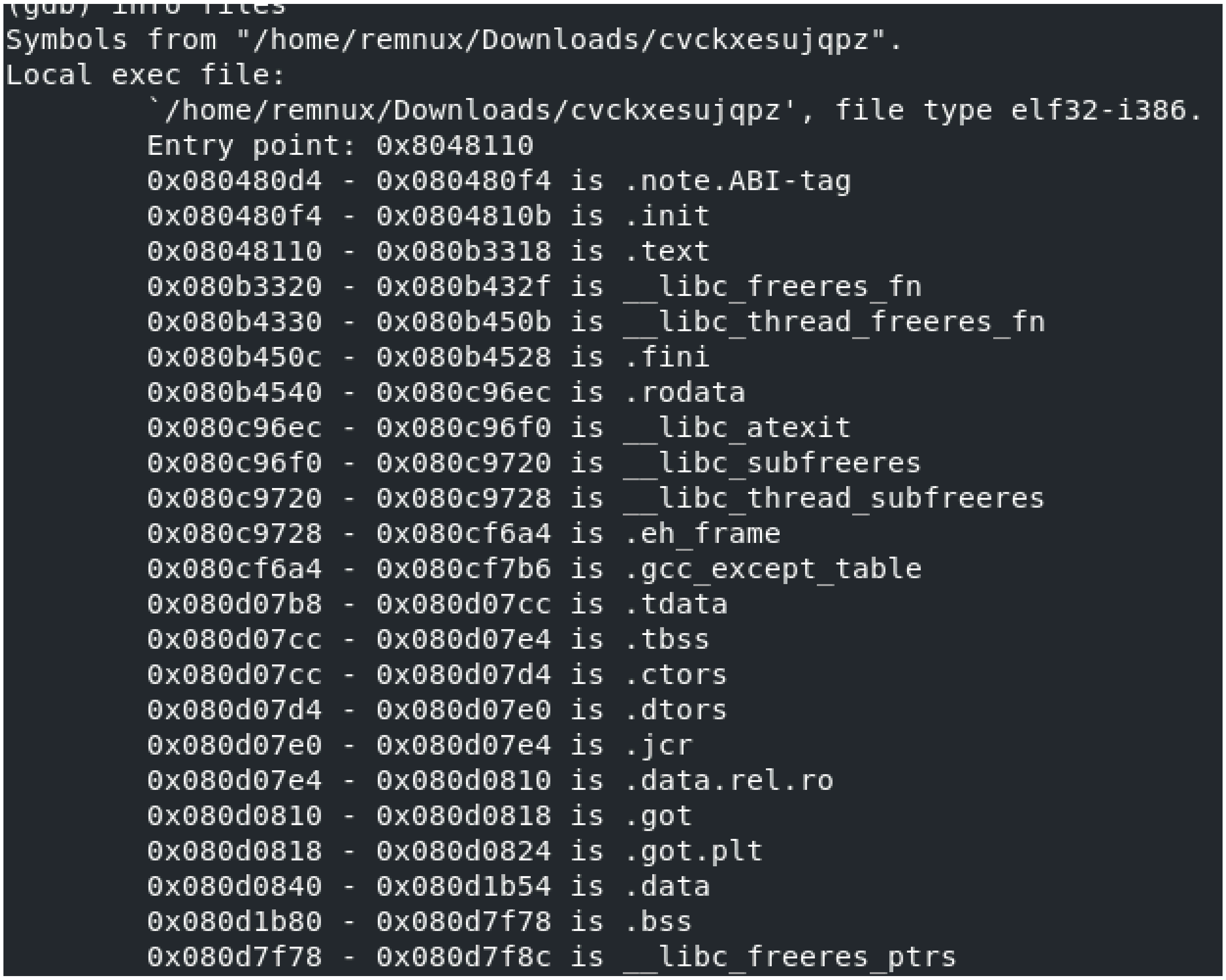
Selection:0000000000000000 Size:0000000000000001



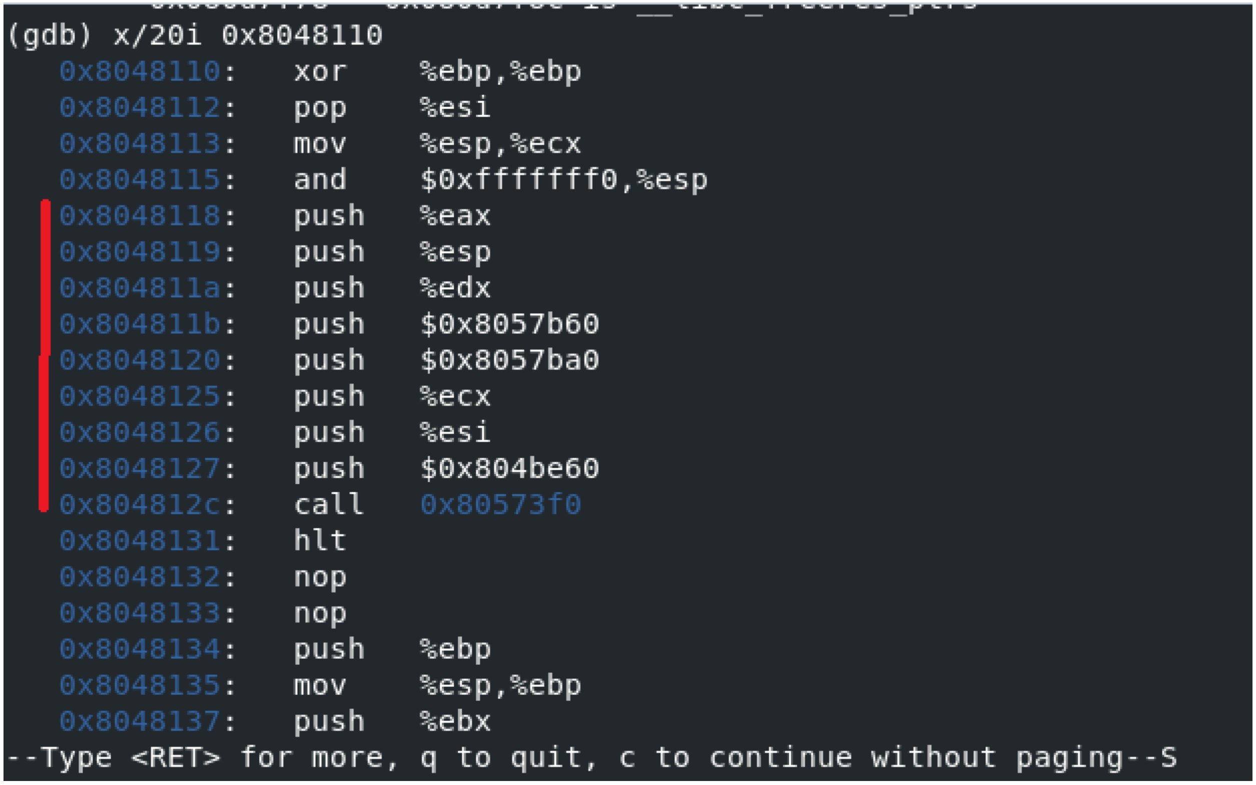
```
(gdb) quit
remnux@remnux:~/Downloads$ file cvckxesujqpz
cvckxesujqpz: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, stripped
remnux@remnux:~/Downloads$ gdb cvckxesujqpz
```



```
  [Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
  [ 0]                   NULL            00000000 000000 000000 00      0   0  0
  [ 1] .note.ABI-tag     NOTE            080480d4 0000d4 000020 00   A  0   0  4
  [ 2] .init             PROGBITS        080480f4 0000f4 000017 00  AX  0   0  4
  [ 3] .text             PROGBITS        08048110 000110 06b208 00  AX  0   0 16
  [ 4] __libc_freeres_fn PROGBITS        080b3320 06b320 00100f 00  AX  0   0 16
  [ 5] __libc_thread_fre PROGBITS        080b4330 06c330 0001db 00  AX  0   0 16
  [ 6] .fini             PROGBITS        080b450c 06c50c 00001c 00  AX  0   0  4
  [ 7] .rodata           PROGBITS        080b4540 06c540 0151ac 00   A  0   0 32
  [ 8] __libc_atexit     PROGBITS        080c96ec 0816ec 000004 00   A  0   0  4
  [ 9] __libc_subfreeres PROGBITS        080c96f0 0816f0 000030 00   A  0   0  4
  [10] __libc_thread_sub PROGBITS        080c9720 081720 000008 00   A  0   0  4
  [11] .eh_frame         PROGBITS        080c9728 081728 005f7c 00   A  0   0  4
  [12] .gcc_except_table PROGBITS        080cf6a4 0876a4 000112 00   A  0   0  1
  [13] .tdata            PROGBITS        080d07b8 0877b8 000014 00 WAT  0   0  4
  [14] .tbss             NOBITS          080d07cc 0877cc 000018 00 WAT  0   0  4
  [15] .ctors            PROGBITS        080d07cc 0877cc 000008 00  WA  0   0  4
  [16] .dtors            PROGBITS        080d07d4 0877d4 00000c 00  WA  0   0  4
  [17] .jcr              PROGBITS        080d07e0 0877e0 000004 00  WA  0   0  4
  [18] .data.rel.ro      PROGBITS        080d07e4 0877e4 00002c 00  WA  0   0  4
  [19] .got              PROGBITS        080d0810 087810 000008 04  WA  0   0  4
  [20] .got.plt          PROGBITS        080d0818 087818 00000c 04  WA  0   0  4
  [21] .data             PROGBITS        080d0840 087840 001314 00  WA  0   0 64
  [22] .bss              NOBITS          080d1b80 088b54 0063f8 00  WA  0   0 64
  [23] __libc_freeres_pt NOBITS          080d7f78 088b54 000014 00  WA  0   0  4
  [24] .comment          PROGBITS        00000000 088b54 0003c6 00      0   0  1
  [25] .shstrtab         STRTAB          00000000 088f1a 000116 00      0   0  1
```



```
(gdb) info files
Symbols from "/home/remnux/Downloads/cvckxesujqpz".
Local exec file:
        `/home/remnux/Downloads/cvckxesujqpz', file type elf32-i386.
        Entry point: 0x8048110
        0x080480d4 - 0x080480f4 is .note.ABI-tag
        0x080480f4 - 0x0804810b is .init
        0x08048110 - 0x080b3318 is .text
        0x080b3320 - 0x080b432f is __libc_freeres_fn
        0x080b4330 - 0x080b450b is __libc_thread_freeres_fn
        0x080b450c - 0x080b4528 is .fini
        0x080b4540 - 0x080c96ec is .rodata
        0x080c96ec - 0x080c96f0 is __libc_atexit
        0x080c96f0 - 0x080c9720 is __libc_subfreeres
        0x080c9720 - 0x080c9728 is __libc_thread_subfreeres
        0x080c9728 - 0x080cf6a4 is .eh_frame
        0x080cf6a4 - 0x080cf7b6 is .gcc_except_table
        0x080d07b8 - 0x080d07cc is .tdata
        0x080d07cc - 0x080d07e4 is .tbss
        0x080d07cc - 0x080d07d4 is .ctors
        0x080d07d4 - 0x080d07e0 is .dtors
        0x080d07e0 - 0x080d07e4 is .jcr
        0x080d07e4 - 0x080d0810 is .data.rel.ro
        0x080d0810 - 0x080d0818 is .got
        0x080d0818 - 0x080d0824 is .got.plt
        0x080d0840 - 0x080d1b54 is .data
        0x080d1b80 - 0x080d7f78 is .bss
        0x080d7f78 - 0x080d7f8c is __libc_freeres_ptrs
```



```
    0x080a77f8 - 0x080a780c is __libc_freeres_ptrs
(gdb) x/20i 0x8048110
   0x8048110:   xor    %ebp,%ebp
   0x8048112:   pop    %esi
   0x8048113:   mov    %esp,%ecx
   0x8048115:   and    $0xfffffff0,%esp
   0x8048118:   push   %eax
   0x8048119:   push   %esp
   0x804811a:   push   %edx
   0x804811b:   push   $0x8057b60
   0x8048120:   push   $0x8057ba0
   0x8048125:   push   %ecx
   0x8048126:   push   %esi
   0x8048127:   push   $0x804be60
   0x804812c:   call   0x80573f0
   0x8048131:   hlt
   0x8048132:   nop
   0x8048133:   nop
   0x8048134:   push   %ebp
   0x8048135:   mov    %esp,%ebp
   0x8048137:   push   %ebx
--Type <RET> for more, q to quit, c to continue without paging--S
```

```
find / | grep -v ‘^proc’ > snap1
Chmod 777 “MyElf.elf”
//Run it
find / | grep -v ‘^proc’ > snap2
diff -crB snap1 snap2 > list_of_dropped_files.txt
```

```
Strace “MyElf.elf” -o dump.txt
```