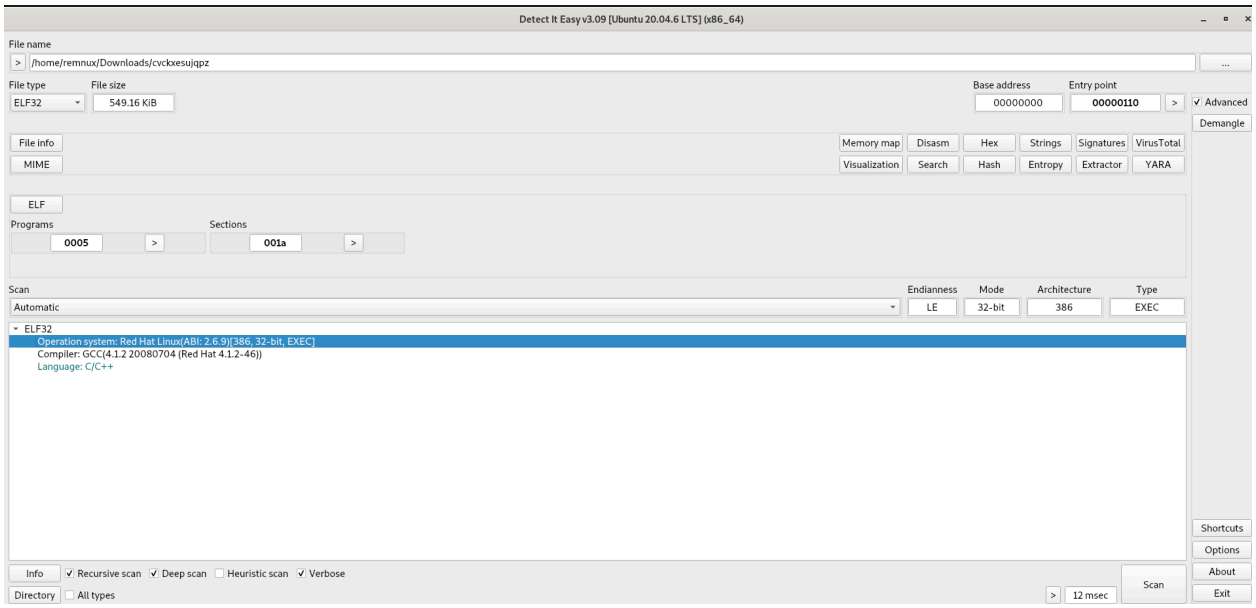

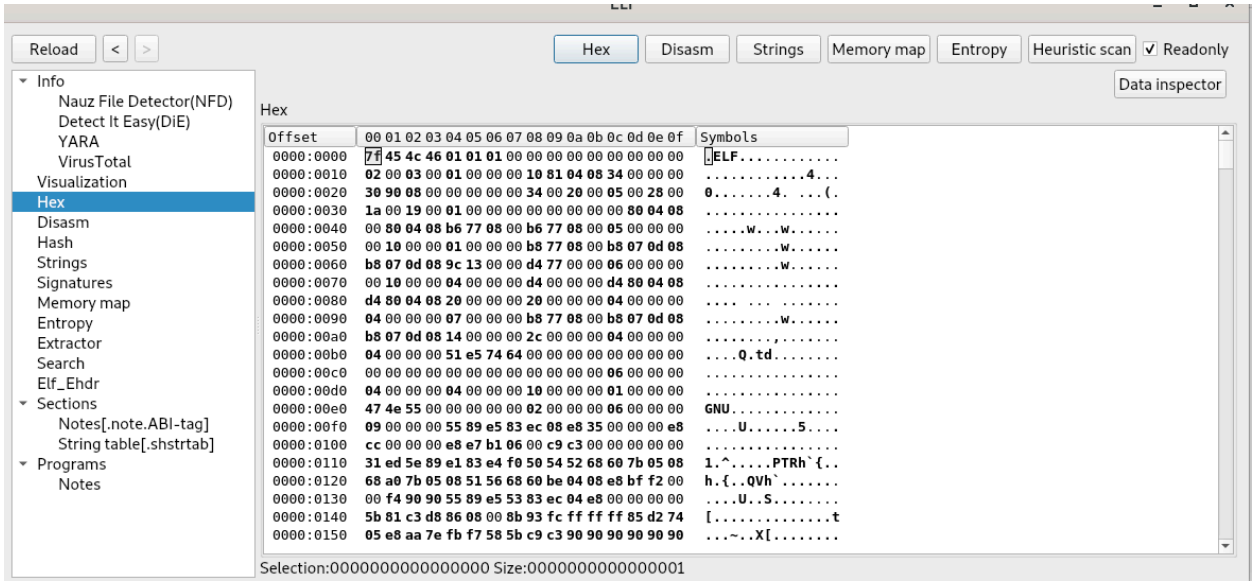


```
(gdb) quit
remnux@remnux:~/Downloads$ file cvckxesujqpz
cvckxesujqpz: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, stripped
remnux@remnux:~/Downloads$ gdb cvckxesujqpz
```

Readelf -a “MyElf.elf”

```
[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
```

Info files

```
(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
```

x/20i address or x/220i $eip

```
(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
```

```
(gdb) x/15i $eip
=> 0x8057510:   movb   $0xff,-0xd(%ebp)
   0x8057514:   lea    -0x10(%ebp),%ecx
   0x8057517:   movb   $0xa,-0xe(%ebp)
   0x805751b:   xor    -0x10(%ebp),%eax
   0x805751e:   and    $0x7ffff0,%ecx
   0x8057524:   add    %gs:0x0,%edx
   0x805752b:   shl    $0x9,%ecx
   0x805752e:   and    $0x7fff00,%edx
   0x8057534:   xor    %ecx,%eax
   0x8057536:   shl    $0x3,%edx
   0x8057539:   xor    %edx,%eax
   0x805753b:   mov    %eax,-0x10(%ebp)
   0x805753e:   mov    %eax,%gs:0x14
   0x8057544:   mov    0x1c(%ebp),%ebx
   0x8057547:   test   %ebx,%ebx
```

```
80574fd:       0f b7 c3                movzx  eax,bx
8057500:       c7 c2 e8 ff ff ff       mov    edx,0xffffffe8
8057506:       c7 45 f0 00 00 00 00    mov    DWORD PTR [ebp-0x10],0x0
805750d:       c1 e0 08                shl    eax,0x8
8057510:       c6 45 f3 ff             mov    BYTE PTR [ebp-0xd],0xff
8057514:       8d 4d f0                lea    ecx,[ebp-0x10]
8057517:       c6 45 f2 0a             mov    BYTE PTR [ebp-0xe],0xa
805751b:       33 45 f0                xor    eax,DWORD PTR [ebp-0x10]
805751e:       81 e1 f0 ff 7f 00       and    ecx,0x7ffff0
8057524:       65 03 15 00 00 00 00    add    edx,DWORD PTR gs:0x0
805752b:       c1 e1 09                shl    ecx,0x9
805752e:       81 e2 00 ff 7f 00       and    edx,0x7fff00
8057534:       31 c8                   xor    eax,ecx
8057536:       c1 e2 03                shl    edx,0x3
8057539:       31 d0                   xor    eax,edx
805753b:       89 45 f0                mov    DWORD PTR [ebp-0x10],eax
805753e:       65 a3 14 00 00 00       mov    gs:0x14,eax
8057544:       8b 5d 1c                mov    ebx,DWORD PTR [ebp+0x1c]
8057547:       85 db                   test   ebx,ebx
8057549:       74 1b                   je     0x8057566
```

```
Breakpoint 1, 0x0804be8e in ?? ()
(gdb) x/20i $eip
=> 0x804be8e:   call   0x806ccd0
   0x804be93:   movl   $0x1,0x4(%esp)
   0x804be9b:   movl   $0x16,(%esp)
   0x804bea2:   call   0x8057d80
   0x804bea7:   movl   $0x1,0x4(%esp)
   0x804beaf:   movl   $0x15,(%esp)
   0x804beb6:   call   0x8057d80
   0x804bebb:   movl   $0x1,0x4(%esp)
   0x804bec3:   movl   $0x14,(%esp)
   0x804beca:   call   0x8057d80
   0x804becf:   movl   $0x1,0x4(%esp)
   0x804bed7:   movl   $0x1,(%esp)
   0x804bede:   call   0x8057d80
   0x804bee3:   movl   $0x1,0x4(%esp)
   0x804beeb:   movl   $0xd,(%esp)
   0x804bef2:   call   0x8057d80
   0x804bef7:   movl   $0x1,0x4(%esp)
   0x804beff:   movl   $0x11,(%esp)
   0x804bf06:   call   0x8057d80
   0x804bf0b:   mov    -0x30(%ebp),%edx
(gdb)
```

```
> 0x806ccd0:   push   %ebp
  0x806ccd1:   mov    %esp,%ebp
  0x806ccd3:   push   %ebx
  0x806ccd4:   sub    $0x6c,%esp
  0x806ccd7:   call   0x8052e50
  0x806ccdc:   cmp    $0xffffffff,%eax
  0x806ccdf:   je     0x806cd20
  0x806cce1:   test   %eax,%eax
  0x806cce3:   jne    0x806cd10
  0x806cce5:   call   0x806a0a0
  0x806ccea:   add    $0x1,%eax
  0x806cced:   lea    0x0(%esi),%esi
  0x806ccf0:   je     0x806cd20
  0x806ccf2:   mov    0x8(%ebp),%edx
  0x806ccf5:   test   %edx,%edx
  0x806ccf7:   je     0x806cdb7
  0x806ccfd:   mov    0xc(%ebp),%eax
  0x806cd00:   test   %eax,%eax
  0x806cd02:   je     0x806cd30
  0x806cd04:   add    $0x6c,%esp
(gdb)
```

```
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
```