**Malwareanalyse und Reverseengineering: Praktikumsaufgabe 1**

**1.4 Programm übersetzen und analysieren**

a, In welchen ELF-Sektionen liegen die Variablen a, b und c?

**Nötige Befehle:**

* gcc -o foobar.o foobar.c (Objektdatei foobar.o erstellen)
* ./foobar.o ; echo $? (Returnwert von Main ausgeben lassen, hier: 20)
* readelf -S foobar.o (Sektions-Header anzeigen)
* hexdump -C foobar.o (Hexdump anzeigen)
* nm foobar.o (Zuordnung von Adressen in ausführbarer Datei zu Variablennamen)

**Variable a** ist eine globale, vorinitialisierte konstante Variable mit Wert 42

Sektion: .rodata, Adresse: 0x004005f4, Wert: 2a

**Variable b** ist eine globale, vorinitialisierte Variable mit Wert 43

Sektion: .data, Adresse 0x00601038, Wert: 2b

**Variable c** ist eine globale, uninitialisierte Variable

Sektion: .bss, ab Adresse 0x00601050, Wert: 75 62 75 6e

b, Was fällt Ihnen bei der Variable “counter” auf? Was könnte der Grund für diesen Effekt sein?

**Beobachtung:** Die Variable Counter taucht sowohl in Adresse 0x00601048 als auch in Adresse 0x0060104c auf. Sie ist also zweimal vorhanden!

**Erklärung:** Im Programm wird die Variable „counter“ in zwei unterschiedlichen Namensräumen definiert, daher befindet sie sich auch zweimal im Speicher.

c, An welchen Adressen liegen die einzelnen ELF-Sektionen?

(Befehl: nm foobar.o)

**Sektions-Header:**

[Nr] Name Typ Adresse Offset

Größe Eintragsgröße Flags Link Info Ausr.

[ 0] NULL 0000000000000000 00000000

0000000000000000 0000000000000000 0 0 0

[ 1] .interp PROGBITS 0000000000400238 00000238

000000000000001c 0000000000000000 A 0 0 1

[ 2] .note.ABI-tag NOTE 0000000000400254 00000254

0000000000000020 0000000000000000 A 0 0 4

[ 3] .note.gnu.build-i NOTE 0000000000400274 00000274

0000000000000024 0000000000000000 A 0 0 4

[ 4] .gnu.hash GNU\_HASH 0000000000400298 00000298

000000000000001c 0000000000000000 A 5 0 8

[ 5] .dynsym DYNSYM 00000000004002b8 000002b8

0000000000000048 0000000000000018 A 6 1 8

[ 6] .dynstr STRTAB 0000000000400300 00000300

0000000000000038 0000000000000000 A 0 0 1

[ 7] .gnu.version VERSYM 0000000000400338 00000338

0000000000000006 0000000000000002 A 5 0 2

[ 8] .gnu.version\_r VERNEED 0000000000400340 00000340

0000000000000020 0000000000000000 A 6 1 8

[ 9] .rela.dyn RELA 0000000000400360 00000360

0000000000000018 0000000000000018 A 5 0 8

[10] .rela.plt RELA 0000000000400378 00000378

0000000000000030 0000000000000018 A 5 12 8

[11] .init PROGBITS 00000000004003a8 000003a8

000000000000001a 0000000000000000 AX 0 0 4

[12] .plt PROGBITS 00000000004003d0 000003d0

0000000000000030 0000000000000010 AX 0 0 16

[13] .text PROGBITS 0000000000400400 00000400

00000000000001e2 0000000000000000 AX 0 0 16

[14] .fini PROGBITS 00000000004005e4 000005e4

0000000000000009 0000000000000000 AX 0 0 4

[15] .rodata PROGBITS 00000000004005f0 000005f0

0000000000000008 0000000000000000 A 0 0 4

[16] .eh\_frame\_hdr PROGBITS 00000000004005f8 000005f8

0000000000000044 0000000000000000 A 0 0 4

[17] .eh\_frame PROGBITS 0000000000400640 00000640

000000000000013c 0000000000000000 A 0 0 8

[18] .init\_array INIT\_ARRAY 0000000000600e10 00000e10

0000000000000008 0000000000000000 WA 0 0 8

[19] .fini\_array FINI\_ARRAY 0000000000600e18 00000e18

0000000000000008 0000000000000000 WA 0 0 8

[20] .jcr PROGBITS 0000000000600e20 00000e20

0000000000000008 0000000000000000 WA 0 0 8

[21] .dynamic DYNAMIC 0000000000600e28 00000e28

00000000000001d0 0000000000000010 WA 6 0 8

[22] .got PROGBITS 0000000000600ff8 00000ff8

0000000000000008 0000000000000008 WA 0 0 8

[23] .got.plt PROGBITS 0000000000601000 00001000

0000000000000028 0000000000000008 WA 0 0 8

[24] .data PROGBITS 0000000000601028 00001028

0000000000000014 0000000000000000 WA 0 0 8

[25] .bss NOBITS 000000000060103c 0000103c

000000000000001c 0000000000000000 WA 0 0 4

[26] .comment PROGBITS 0000000000000000 0000103c

000000000000002b 0000000000000001 MS 0 0 1

[27] .shstrtab STRTAB 0000000000000000 00001067

0000000000000108 0000000000000000 0 0 1

[28] .symtab SYMTAB 0000000000000000 000018f0

00000000000006d8 0000000000000018 29 47 8

[29] .strtab STRTAB 0000000000000000 00001fc8

0000000000000257 0000000000000000 0 0 1