Lab 7: ELF

Task 0a

1. ELF header, 0x80482e0 (readelf -h)
2. 34
3. 1b8 (readelf -a)
4. 080482e0 (readelf -s)
5. 08048388
6. section_file_offset + function_virtual_address - section_virtual_address
   * typeof main is func

Task 1b

In our program we print out a number, and in hexedit it is printed according to little endian.

Task 2a

1. run
2. _start
3. 08048156

```
Num:    Value  Size Type    Bind   Vis      Ndx Name
8:      08048156     0 NOTYPE  GLOBAL DEFAULT    2 _start
```

Task 2b

What are the values of location/length? How do you know that?

Entry point address: 0x804816c

not sure…

24 (decimal) = 18 (hexa)

location = 18 ??

length = 1 (assuming unit_size = 4)

Task 3a

65: 08048464   175 FUNC   GLOBAL DEFAULT   13 main

offset of main: 08048464

Size: 175 (decimal)

[13] .text   PROGBITS   080483b0 0003b0 00020c 00 AX 0 0 16

.text offset: 3b0

.text size: 20c

.text address: 080483b0

main offset within the .text: 08048464-080483b0 = b4 (180 decimal)

main offset within the file: 08048464-080483b0+3b0 = 464 (1162 decimal)

Task 3b

https://c9x.me/x86/html/file_module_x86_id_270.html
understood by the opcode...

Task 4

The problem with ntsc is that it only counts digits 1-8 (not 0,9)
readelf -a ntsc

```
NUM Value       Size   Type      Bind       Vis            Ndx   Name
68: 00000577  1136 FUNC    GLOBAL DEFAULT   14 digit_cnt
69: 000004ed   80    FUNC    GLOBAL DEFAULT   14 digit_cnt
```

```
[Nr] Name           Type               Addr          Off        Size        ES  Flg Lk Inf Al
[14] .text          PROGBITS        00000410 000410 0006b2 00  AX  0    0 16
[14] .text          PROGBITS        000003b0 0003b0 000212 00  AX  0    0 16
```

digit_cnt offset within the .text: 410- 00000410 = 0
digit_cnt offset within the file: 000410

```
caspl202@caspl202-lubuntu:~/Desktop/labs/lab7/Task4$ ./hexeditplus
choose action: ...
Option: 2
Enter new unit size:
1
Option: 1
Enter new file name:
digit_cnt
Option: 3
Please enter <location> <length>:
4ed 80
file name: digit_cnt
location: 1261
length: 80
Loaded 80 units into memory
Option: 1
Enter new file name:
ntsc
Option: 5
Please enter <source-address> <target-location> <length>:
0 577 80
Option: 7
quitting
```

```
caspl202@caspl202-lubuntu:~/Desktop/labs/lab7/Task4$ ./ntsc 09
The number of digits in the string is: 2
```