Lab 7: ELF

Task0a

1. ELF header, 0x80482e0
2. 33 / 34 (does NULL count?)
3. 18b
4. 080482e0 (\ text section (12)?)
5. 08048388 (\ text section (12)?)
6. ?

* typeof main is func
* text offset is 02e0, and its' size is 1b8

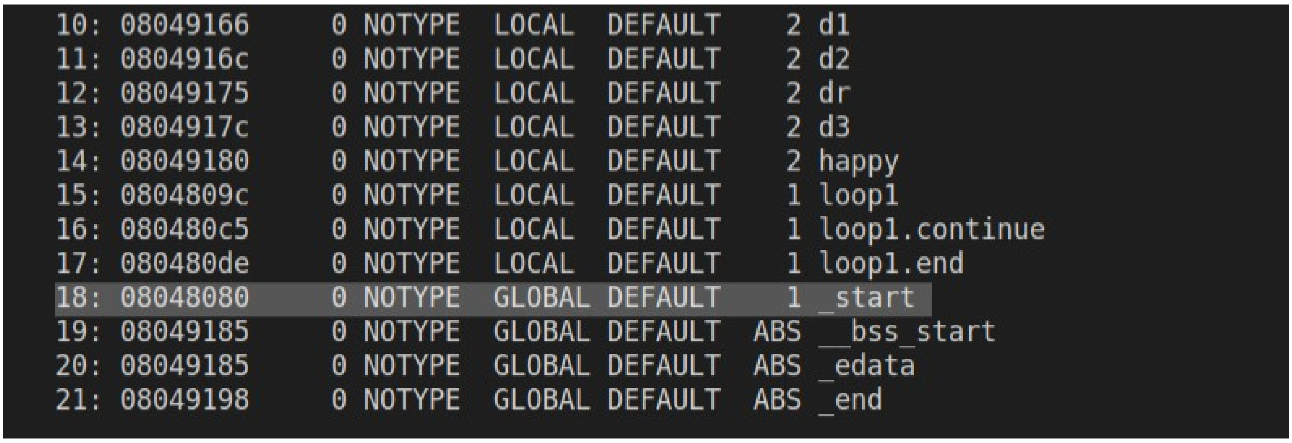
Task1c

Note that, depending on the chosen unit size, the printed hexadecimal values may differ in order when compared with the output of *hexedit*. Why is that?

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

Task2a

2. _start
3. 8048080. entry point is at 804808a



```
    10: 08049166     0 NOTYPE  LOCAL  DEFAULT    2 d1
    11: 0804916c     0 NOTYPE  LOCAL  DEFAULT    2 d2
    12: 08049175     0 NOTYPE  LOCAL  DEFAULT    2 dr
    13: 0804917c     0 NOTYPE  LOCAL  DEFAULT    2 d3
    14: 08049180     0 NOTYPE  LOCAL  DEFAULT    2 happy
    15: 0804809c     0 NOTYPE  LOCAL  DEFAULT    1 loop1
    16: 080480c5     0 NOTYPE  LOCAL  DEFAULT    1 loop1.continue
    17: 080480de     0 NOTYPE  LOCAL  DEFAULT    1 loop1.end
    18: 08048080     0 NOTYPE  GLOBAL DEFAULT    1 _start
    19: 08049185     0 NOTYPE  GLOBAL DEFAULT  ABS __bss_start
    20: 08049185     0 NOTYPE  GLOBAL DEFAULT  ABS _edata
    21: 08049198     0 NOTYPE  GLOBAL DEFAULT  ABS _end
```

Task2b

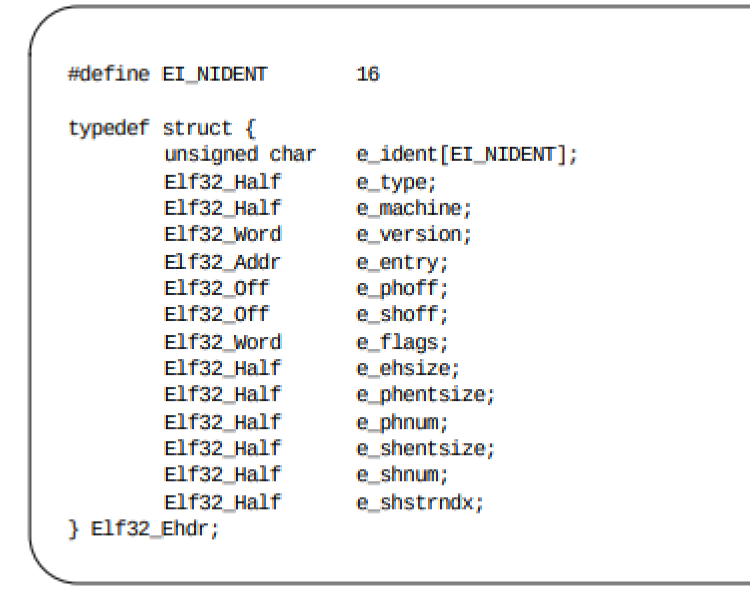
What are the values of location/length? How do you know that?

28 (decimal) = 18 (hexa)

location = 18

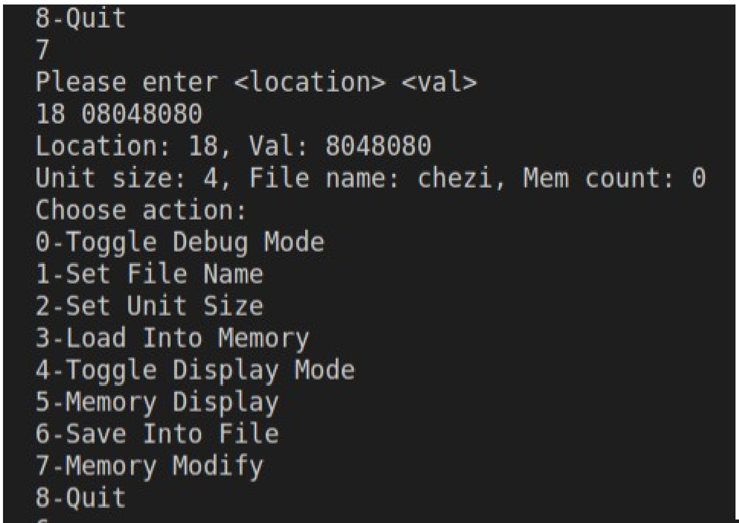
length = 1 (assumint unit_size = 4)

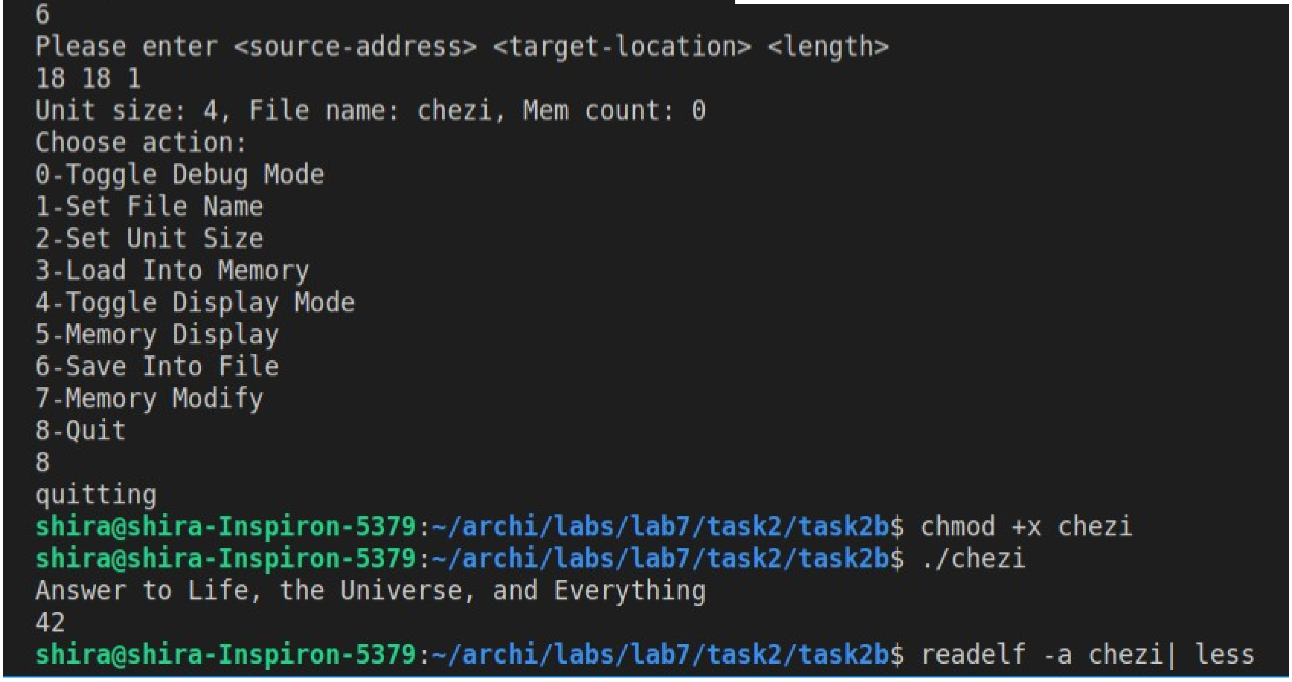
Figure 1-3: ELF Header



```
#define EI_NIDENT       16

typedef struct {
        unsigned char   e_ident[EI_NIDENT];
        Elf32_Half      e_type;
        Elf32_Half      e_machine;
        Elf32_Word      e_version;
        Elf32_Addr      e_entry;
        Elf32_Off       e_phoff;
        Elf32_Off       e_shoff;
        Elf32_Word      e_flags;
        Elf32_Half      e_ehsize;
        Elf32_Half      e_phentsize;
        Elf32_Half      e_phnum;
        Elf32_Half      e_shentsize;
        Elf32_Half      e_shnum;
        Elf32_Half      e_shstrndx;
} Elf32_Ehdr;
```





```
8-Quit
7
Please enter <location> <val>
18 08048080
Location: 18, Val: 8048080
Unit size: 4, File name: chezi, Mem count: 0
Choose action:
0-Toggle Debug Mode
1-Set File Name
2-Set Unit Size
3-Load Into Memory
4-Toggle Display Mode
5-Memory Display
6-Save Into File
7-Memory Modify
8-Quit
6
Please enter <source-address> <target-location> <length>
18 18 1
Unit size: 4, File name: chezi, Mem count: 0
Choose action:
0-Toggle Debug Mode
1-Set File Name
2-Set Unit Size
3-Load Into Memory
4-Toggle Display Mode
5-Memory Display
6-Save Into File
7-Memory Modify
8-Quit
8
quitting
shira@shira-Inspiron-5379:~/archi/labs/lab7/task2/task2b$ chmod +x chezi
shira@shira-Inspiron-5379:~/archi/labs/lab7/task2/task2b$ ./chezi
Answer to Life, the Universe, and Everything
42
shira@shira-Inspiron-5379:~/archi/labs/lab7/task2/task2b$ readelf -a chezi| less
```

Task3a

Entry point for main: 08048464
Size: 175 (decimal)
.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)

Task3b
https://c9x.me/x86/html/file_module_x86_id_270.html

Task 4

The problem with ntsc is that it only counts digits 1-8 (0 and 9 are not counted)

ntsc

Entry point address: 0x410

NUM	Value	Size	Type	Bind	Vis	Ndx	Name
68:	00000577	1136	FUNC	GLOBAL	DEFAULT	14 (.text)	digit_cnt
69:	000004ed	67	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	16q

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

task4 code

```
Choose action:...
0
Debug flag now on
Unit size: 1, File name: , Mem count: 0
Choose action:...
8-Quit
1
Please enter the file name: task4
Unit size: 1, File name: task4, Mem count: 0
Choose action:...
3
Please enter <location> <length>
4ed 67
File name: task4
Location: 4ED
Length: 67
Loaded 67 units into memory
Unit size: 1, File name: task4, Mem count: 0
Choose action:...
1
Please enter the file name: ntsc
Unit size: 1, File name: ntsc, Mem count: 0
Choose action:...
6
Please enter <source-address> <target-location> <length>
0 577 67
Unit size: 1, File name: ntsc, Mem count: 0
Choose action:...
8
quitting

shira@shira-Inspiron-5379:~/archi/labs/lab7/task4$ ./ntsc 09
The number of digits in the string is: 2
```