Zadanie 4. Opisz znaczenie pól nagłówka ELF «Elf64\_Ehdr» [2, 4-3] oraz tablicy rekordów nagłówków programu «Elf64\_Phdr» [2, 5-1], zwanych również segmentami programu. Na podstawie zdobytej wiedzy omów wydruk polecenia «readelf -h -l» na pliku «mismatch». Skąd wiadomo gdzie znajduje się pierwsza instrukcja pliku wykonywalnego [1, §7.8]? Czy to będzie początek funkcji «main»? Pod jakie adresy wirtualne zostaną załadowane poszczególne segmenty programu? Które z sekcji ne zostaną załadowane do pamięci? Z których sekcji procesor będzie mógł wyłącznie czytać?

```
symbolizuje, że plik jest
ELF'em
typedef struct {
                                 e_ident[EI NIDENT]
          unsigned char
                                 e_type; - typ pliku (relokowalny, wykonywalny, itp.)
          Elf64 Half
                                 e_machine; ~ architectura systemu wymagana do pliku
           Elf64 Half
                                e_version; ~ wersja pliku
e_entry; ~ adres pierwszej instrukcji
          Elf64 Word
          Elf64 Addr
          Elf64_0ff
                                e_shoff; offsety tabeli nagiowkow programu/sekcji
e_flags; flagi powiązane z plikiem
e_ehsize; rozmiar nagiowka ELF
e_phentsize; rozmiar elementów tabeli nagiowkow
e_shentsize; ilość nagiwków programy
          Elf64 Off
          Elf64 Word
          Elf64 Half
          Elf64 Half
                               e_phnum; rozmiun eiemeine
e_shentsize; ilość nagłówków
le shnum; progromu
          Elf64 Half
          Elf64 Half
          Elf64 Half
           Elf64 Half
                          to samo d'a tabeli nagiówkow w tabeli nagiówkow sekcji
} Elf64 Ehdr;
```

nogtówek ELF → segment zawierający podstawowe informacje na temat pliku

```
typedef struct {
    Elf64_Word
    Elf64_Word
    Elf64_Off
    Elf64_Addr
    Elf64_Addr
    Elf64_Xword
    Elf64_Xword
    Elf64_Xword
    Elf64_Xword
    Elf64_Phdr;

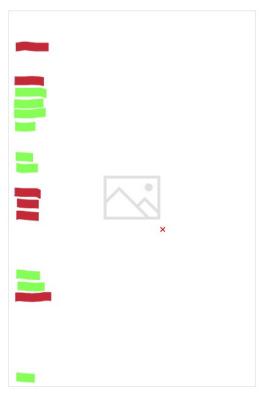
    dig p segmentu

    p segmentu
    p segmentu względem początku
    p offset;
    offset segmentu względem początku
    p offset;
    p offset;
    p offset;
    p offset;
    p odres pierwszego bojtu segmentu w
    p pomięci wirtualnej
    p odres fizyczny (opcjonalnie)
    p memsz;
    p memsz;
    obrazie pliku / obrazie pamięci
    allignment segmentu w pamięci
```

· naglówek programu -> rekord zawierająwy informacje potrzebne systemowi do przygotowania pliky do uruchomienia

adres pierwszej instrukcji znajduje się w nagtówku ELF segmenty są Ladowane zgodnie z polem p-vaddr w odpowiadających im nagtówkach programu

nie zolodowane zostanoz sekcje bez atrybutu shEalloc (pole flags)



- sekije read-only (bez atrybutu shf\_write)