

Task 0a

① entry point הוא offset section header והוא נמצא ב-0x00000000 בכתובת ELF.
 במקרה שלנו, הוא נמצא ב-0x00000000.
 section headers נמצאים ב-0x00000000 בכתובת ELF.

② אנו יודעים את מספר ה-sections של המינימום (section header number)
 שנקרא ב-0x00000000. במקרה שלנו, הוא 0x00000000.

③ כדי למצוא את כתובת ה-section text, אנחנו צריכים להשתמש ב-shstrtab.
 החישוב יהיה: $0x00000000 + 0x00000000 = 0x00000000$.
 section headers כוללים את כתובות ה-sections.
 Section text הוא כתובת ה-section text.
 Section size הוא גודל ה-section.

כדי למצוא את כתובת ה-section text, אנחנו צריכים להשתמש ב-shstrtab.
 Section headers כוללים את כתובות ה-sections.
 Section text הוא כתובת ה-section text.
 Section size הוא גודל ה-section.

0123456789
 10111213141516171819
 20212223242526272829
 3031
 0x1204

offset - 0x00000000
 value = addr
 (value of addr)

כדי למצוא את כתובת ה-section text, אנחנו צריכים להשתמש ב-shstrtab.
 Section headers כוללים את כתובות ה-sections.
 Section text הוא כתובת ה-section text.
 Section size הוא גודל ה-section.

אנו צריכים למצוא את כתובת ה-section text.
 Section size הוא גודל ה-section.

④ סדר 3 הסעיפים הבאים, נרץ gdb את הקוד.
 הוא יספק לנו את כתובת ה-section text.

⑤ המקום של start - 0x00000000

⑥ המקום של main - 0x00000000

⑦ start - 0x00000000

⑧ main - 0x00000000

⑨ $fn_symbol_offset = fn_symbol_VA - text_VA + text_offset$

⑩ $0x00000000 = 0x00000000 - 0x00000000 + 0x00000000$

Task 2a

הערה

① שאלנו את ה-permission של הקובץ (chmod)

② הרישיון של הקובץ 'A' הוא הרשיון

③ הרישיון:
 entry point של 0x00000000
 entry point של 0x00000000
 entry point של 0x00000000

④ הרישיון:
 entry point של 0x00000000
 entry point של 0x00000000
 entry point של 0x00000000

0x00000000

Task 2b

הקוד של הקובץ

הקוד של הקובץ
 entry point של 0x00000000
 entry point של 0x00000000
 entry point של 0x00000000

(56.8 from 60) \times 100 = 6.7% \times 2 = 13.4% \times 2 = 26.8% \times 2 = 53.6%

what are the values of location / length?

```

: main

```

175 : Size

65 : entry

: Section 13 -

```
0003 b0      : offset
```

$$VA_{main} - VAS.13 = 08048464 - 08048360 = 64$$

$$VA_{main} - VAS.13 = 08048464 - 08048360 = 64$$

main R: PCBR offset-7 is b4 ✓

$$360 \div 64 = 464 \text{ : } 277$$

Pointer offset \rightarrow 25 464 516

① 已知

⊖ המידה מקומית היא שהיא לא ספרית והספרות 0, 1, 9.

findige KONS 20 readelf ntsc -a 11577 ①

1136 : {212}

1136 : रिए

section 14

: section 14

410 :offset

410 :offset

נמצא את התקופות הרלוונטיות:

section 14 \bar{A} digit counter \bar{A}

(hexa) $577 - 410 = 167 \rightarrow$ offset \rightarrow 16 bits
digit counter

ה' offset-ו זה הפונקציה offset-ו נחנך

(hexa) $167 + 410 = 577 \rightarrow$ offset = 7
written

- digit counter max, (task 4) life Pano ⊖

80 : 124

520 :VA

section 14 :pol/pw

: Section 14 21px

$$3FO : 107N$$

$$520 - 3F0 = 130 \Rightarrow \text{ה offset של } 2GG \text{ : } 130$$

S2.0 → 'Ink' Asset-1)

Ex 3.2 (1)

2019 - 0

task 4 \approx 100% - 1

(size = 80, offset = 0)	80	first	10000	- 3
		ntsc	10000	- 1
(first block offset = 0)	577	10000 target = 0	(mem buf - on type = 0)	0
		(1st size = 0)	80	826
		! 3018 ← .1 ntsc	80	2500, 1010