**מחשוב זמן אמת**

**תרגיל מספר 5**

במערכת מוגנת x86\_32 מוגנת עם דפדוף ידועים הפרטים הבאים:

1. גרעין מערכת ההפעלה מוצבע ע"י כניסה מספר 10 ב-GDT.
2. הכתובת הלינארית של הכניסה הזו הינה 65616.
3. מבנה הנתונים הגלובלי מוצבע ע"י כניסה מספר 11 ב-GDT.
4. המחסנית הפרטית של הגרעין מוצבע ע"י מספר כניסה 12 ב-GDT.
5. מעבר מתהליך יישום לקוד קריאת מערכת היא ע"י שנוי ה-CS לערך 56.
6. המשתנים הסטטיים ומבני הנתונים הגלובליים של הגרעין נמצאים בכתובות לינאריות 1048576 עד 1060864 ובכתובות פיזיות 131072 עד 143359.
7. טבלת ה-LDT של המערכת תמיד מוצבעת ע"י כניסה מספר 9 ב-GDT.
8. טבלת המשנה השלישית של טבלאות הדפים נמצאת בכתובות פיזיות 20480 עד 24575.
9. הטבלה הזו מוצבעת ע"י כניסה ב-Page Directory הנמצאת בכתובת פיזית 8200-8203.

1. (13 נק') מה אתה יכול להסיק מכל המתואר לעיל על כלל אוגרי המעבד בלי קשר לאיזה קוד רץ?

**תשובה:**

על בסיס הנתונים ניתן להסיק את הדברים הבאים:

* GDTR – טעון ומצביע לטבלת ה-GDT שמכילה דסקריפטורים של מערכת ההפעלה.
* LDTR – טעון עם סלקטור לכניסה 9 ב-GDT שמתארת את טבלת ה-LDT,
* CR0 – מופעלים בו 1=PE ו-1=PG.
* CR3 – חייב להצביע על כתובת פיזית מיושרת ל-4KI של תחילת טבלת ה page directory.

1. (3 נק') מה אתה יכול להסיק בנוסף מכל המתואר לעיל על כלל אוגרי המעבד כאשר הגרעין רץ?

**תשובה:**

כשהגרעין רץ, המעבד נמצא ב-Protected mode עם paging פעיל וב- 0=RING

CR3=0X2000 מצביע לpage directory:

CS=0X50 כניסה 10 – מייצג את קוד הגרעין

DS=0X58 כניסה 11 – מייצג נתונים גלובליים

SS=0X60 כניסה 12 – מייצג את מחסנית הגרעין

LDTR=0X48 כניסה *9* – LDT

קריאות המערכת מתרחשות דרך CALL GATE בכניסה 7 0X38 לאחר המעבר ה-CS נטען לערך 0x50 של הגרעין.

1. (11 נק') מה אתה יכול להסיק על תוכן כניסות מסוימות ב-Descriptor tables?

**תשובה:**

כל descriptor בגודל 8 בתים ומגדיר מקטע בזיכרון,

כניסה 9 (LDT) תכיל את הכתובת הבסיסית והגודל של טבלת הLDT,

כניסה 10 (קוד הגרעין) – תתאר את המקטע הקוד של הגרעין, עם: לפחות 12288, base=0 ,limit לפי צורך

כניסה 11 (נתונים גלובליים) תתאר את מקטע הנתונים, עם:  
לפחות 12288 בתים, ,base=0 limit לפי צורך.  
כניסה 12 (מחסנית הגרעין) גם מקטע נתונים עבור המחסנית, base=0 , limit לפי הצורך.

כמובן שהlimit צריך להיות גדול מספיק (לפחות 12288)

1. (6 נק') מה אתה יכול להסיק על תוכן כניסות מסוימות בטבלאות הדפים?

**תשובה:**

ב-CR3=0X2000 נמצאת כתובת הבסיס של Page directory,

ב-page directory יש כניסה בכתובת 0x8200-0x8203 שמצביע על טבלת דפים בכתובת פיזית 20480 (0x5000).

בטבלת דפים שב-0x5000:  
כל כניסה ממפה דף של 4KiB בתחום לינארי 0x100000-0x103000 אל תחום פיזי 0x20000-0x23000 .

לכל כניסה מוגדרים P=1,R/W=1,U/S=0

גם ל-PDE מוגדר P=1,R/W=1,U/S=0

אין ביט "קריאה" – משתמשים בביט R/W בלבד כדי לאפשר גם כתיבה לגרעין.