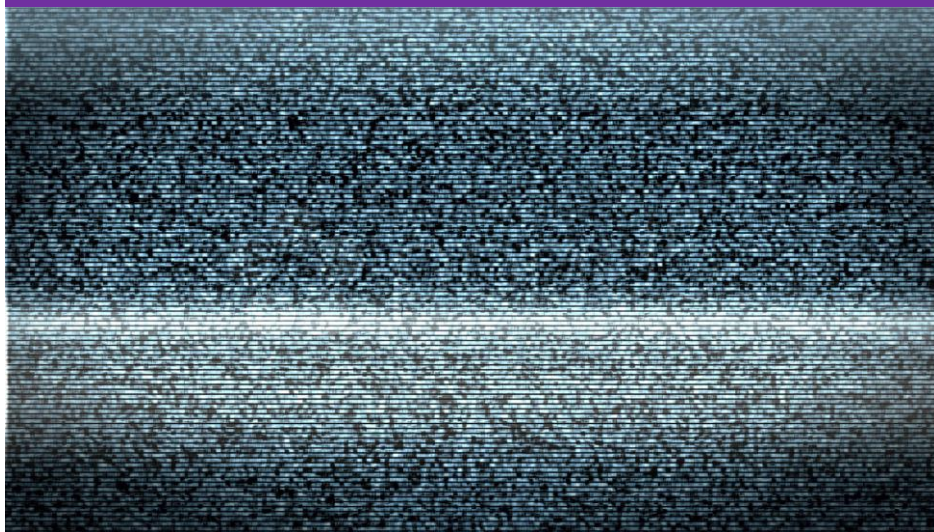




CyberGirlz

☆ CLUB ☆

חלק א - שלג כבד



ברק גונן





קיץ....





לא כולם נחים...
ידוע לנו שמתוכננות מתקפות סייבר מתוחכמות
היעד: אנחנו



מקור מודיעיני שלח לנו מסר מוצפן:

“Winter is coming!

Process Explorer replace Task Manager”

האם תדעו מה לעשות?

זה הזמן לצפות בסרטון ההדרכה



קרדיט:
אלינור תמיר

<https://data.cyber.org.il/CyberGirlzClub/IntroMovie.exe>

נוזקה (Malware)

- תוכנה בעלת לפחות אחת מהמטרות הבאות:

להציג תוכן
פרסומי בלתי-
רצוי

להשיג גישה
לרשתות מחשב
פרטיות

לאסוף מידע
רגיש

לחדור או
להזיק למחשב

- כל זה ללא ידיעתו של המשתמש בה
- המונח "נוזקה" משמש שם כולל לכל סוגי התוכנות שנועדו להזיק למערכת, לחדור אליה או להפריע את פעולתה

מה למדנו עד היום?

ניתוח
פרוטוקולים

תכנות
בשפת פייתון

רשתות וכלים
לניתוח רשת

מה עוד נצטרך ללמוד?

כלים לניתוח
נוזקה

מערכות
הפעלה

הקשר לעולם הסייבר

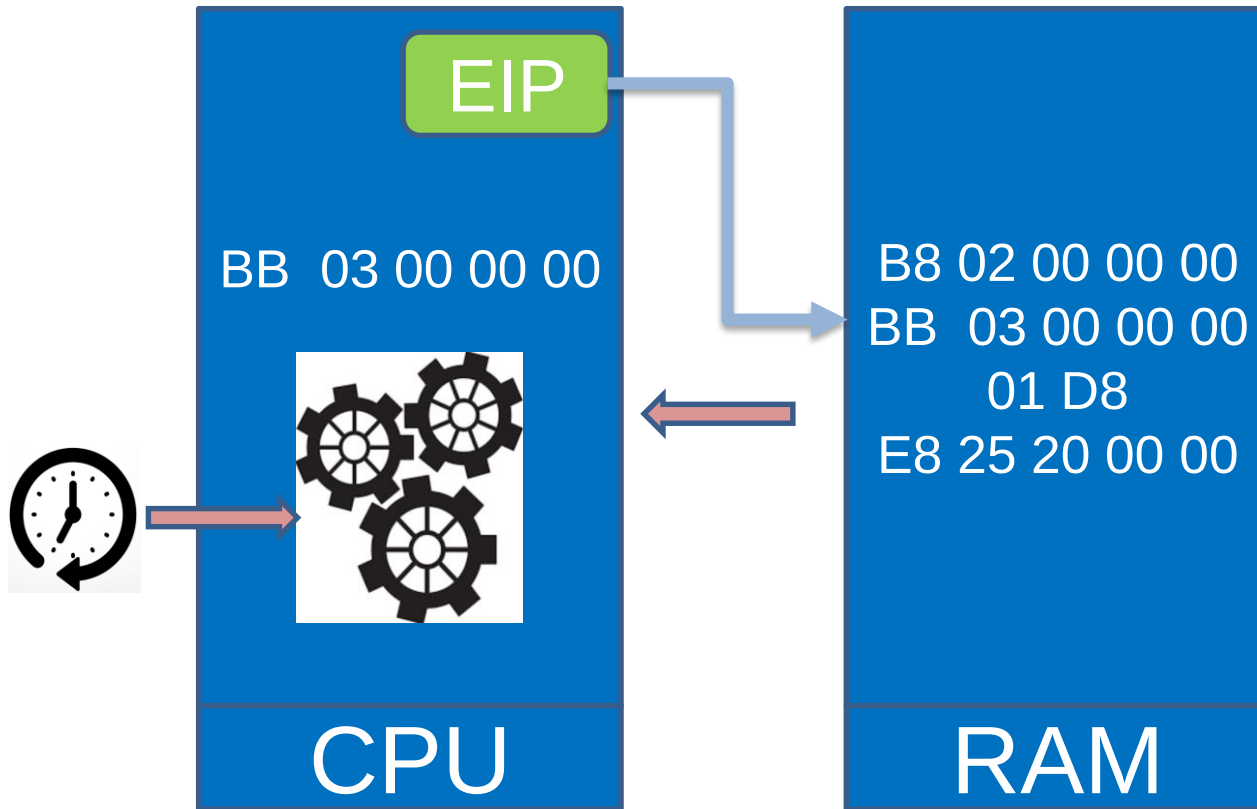
- מערכות הפעלה הן הבסיס שמעליו רצות כל התוכנות במחשב
- תוכנות זדוניות מנצלות פרצות במערכת ההפעלה
- מה תוקפים מנסים להשיג באמצעות מערכת ההפעלה?
 - הרצה של קוד זדוני
 - הקוד יורץ מחדש גם אם המחשב מודלק מחדש
 - הקוד יורץ באופן נסתר בלי לעורר חשד
 - הקוד יאפשר התחברות מרוחקת למחשב
 - הקוד יאפשר חילוץ של מידע מהמחשב – קבצים, סיסמאות וכו
- הגנת סייבר דורשת הבנת מערכת ההפעלה ברמה של התוקפים



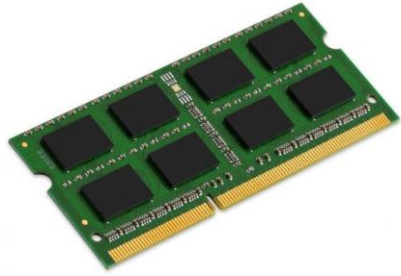
מעבד (CPU)

- Central Processing Unit – CPU (יחידת עיבוד מרכזית)
- רכיב חומרה במחשב, המבצע פקודות המאוחסנות בזיכרון, למשל:
 - קריאת מידע מהזיכרון
 - ביצוע פעולות חשבוניות ולוגיות
 - כתיבת תוצאת החישוב בחזרה לזיכרון

מודל עבודת המעבד



- הפקודות חייבות להיות ב-RAM
- בכל תקתוק של השעון המעבד לוקח את הפקודה שהרגיסטר EIP מצביע עליה ומריץ אותה
- EIP עובר להצביע על הפקודה הבאה



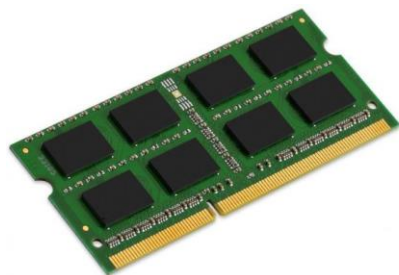
זיכרון (Memory)

מה היינו רוצים מזיכרון?

- מהיר – זמני כתיבה וקריאה קצרים
- גדול – מאחסן את כל הקוד של כל התוכניות
- המידע לא נמחק כשמכבים את המחשב
- זול

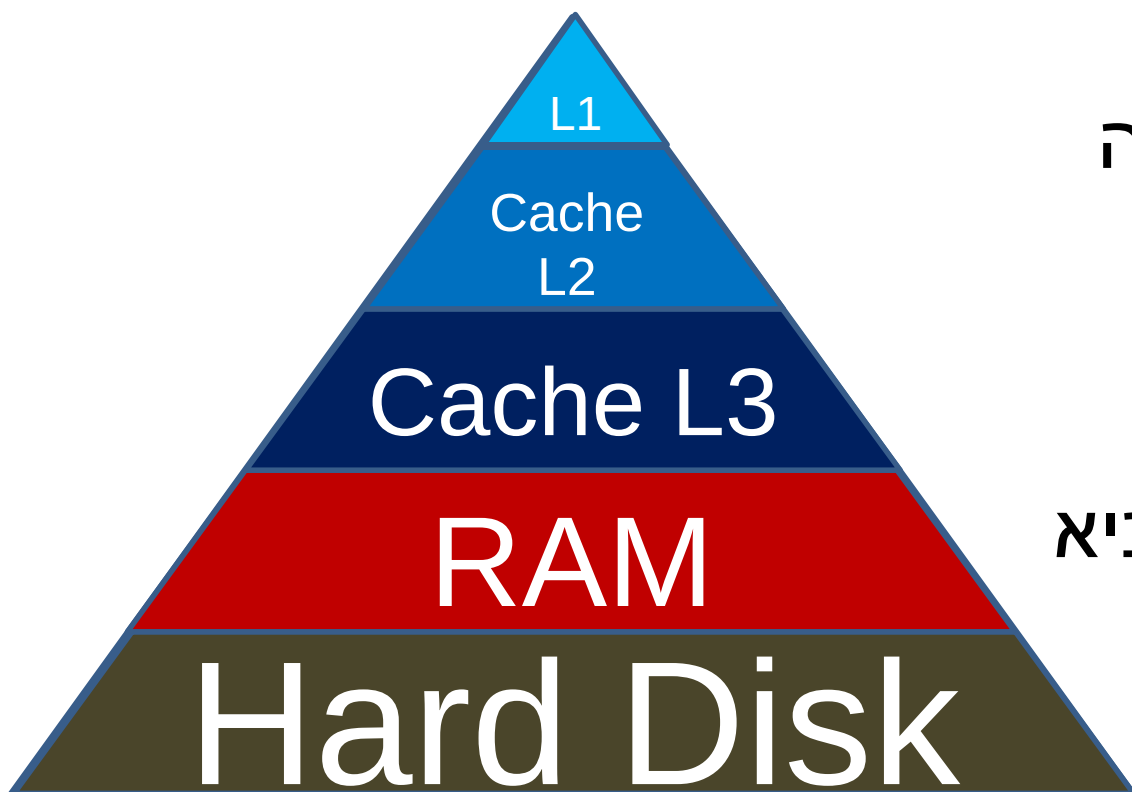
אין דבר כזה ☹️

במחשב יש מספר סוגים של זיכרון, כאשר כל אחד מצטיין במשהו אחר



זיכרון (Memory)

- קיימת היררכיה של זיכרונות – הרבה זיכרון איטי וזול, מעט זיכרון מהיר ויקר
- מערכת ההפעלה שמה קוד ונתונים שימושיים בזיכרון מהיר
- אם מידע אינו נמצא בזיכרון מהיר, יש להביא אותו מזיכרון איטי



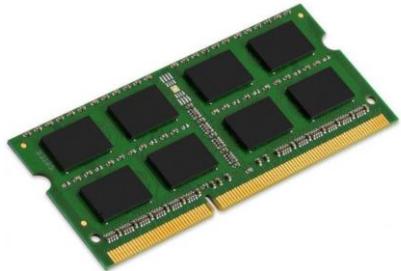
RAM לעומת Hard Disk

RAM	Hard Disk
יקר	זול מאד
מהיר	איטי מאד
נמחק בכיבוי המחשב	לא נמחק בכיבוי המחשב
כמות מועטה	כמות רבה
אפשר להריץ ממנו קוד	אי אפשר להריץ ממנו קוד
המעבד יודע לדבר איתו ישירות	המעבד לא יודע לדבר איתו ישירות

מערכת ההפעלה טוענת ל-RAM את הפקודות של כל process שמופעל

כמה זמן צריך בשביל...

0	• לגשת לרגיסטר –
0.5ns	• לגשת ל-L1 cache –
7ns	• לגשת ל-L2 cache –
100ns	• לגשת ל-RAM –
1,000,000ns	• לגשת לדיסק הקשיח –



המספרים הם הערכות, יכולים להשתנות בין חומרה לחומרה
מקור: <http://norvig.com/21-days.html#answers>

כמה זיכרון יש במחשב שלנו?

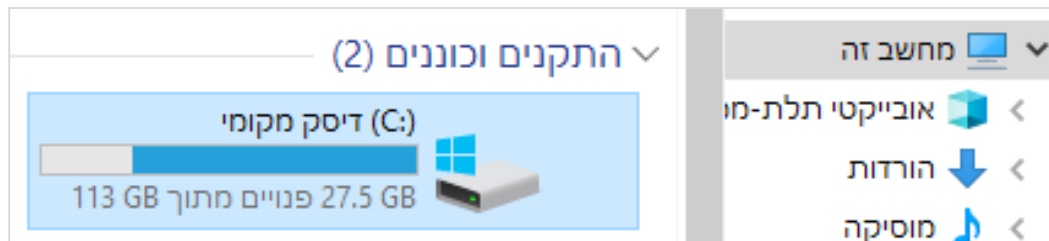
:Hard Disk

בשולחן העבודה, בדקו את גודל



לחצו על

הכוננים שלכן –



:RAM

היכנסו ל- Control Panel ובחרו ב"מערכת" –

מערכת	
מעבד:	Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz 2.20 GHz
זיכרון מותקן (RAM):	8.00 GB (7.89 GB ניתנים לשימוש)

כמה זיכרון יש במחשב שלנו?

- Cache L2, L3: הריצו ב-cmd את הפקודה הבאה-

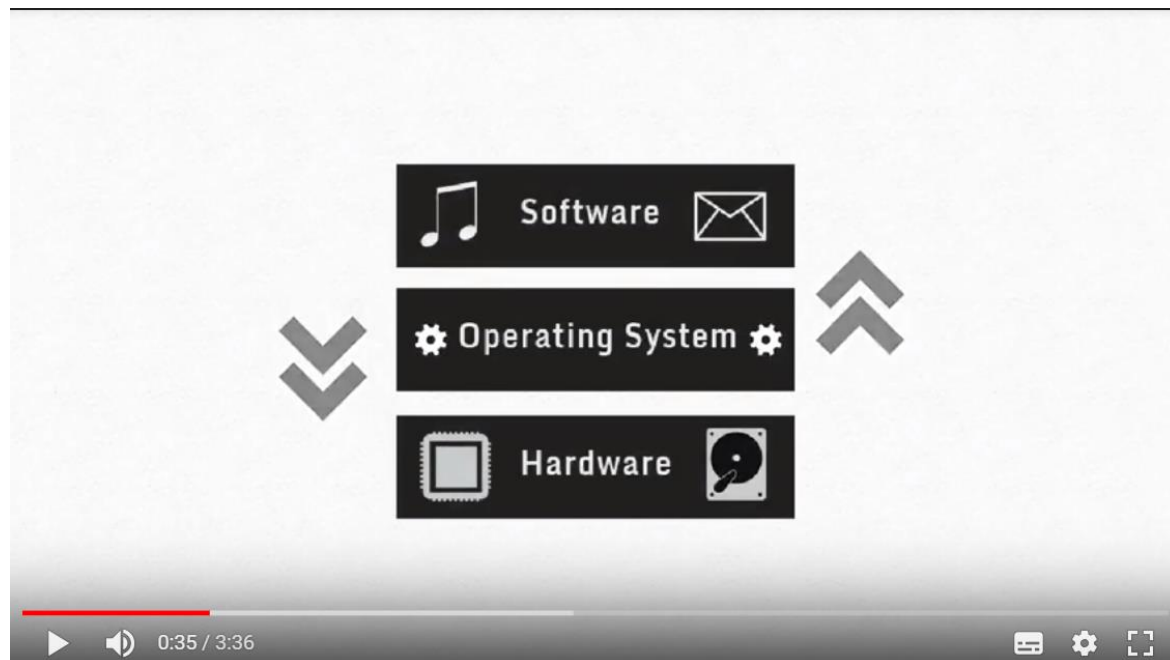
```
wmic cpu get L2CacheSize, L3CacheSize
```

- Cache L1: חפשו ברשת את שם המעבד + L1 cache

 i7 8550u L1 cache

- צפו בסרטון המבואר ושימו לב לארבעת התפקידים

<https://data.cyber.org.il/CyberGirlzClub/IntroMovie.mp4>



תפקידי מערכת ההפעלה

1. ניהול זמן המעבד

- מ"ה קובעת מי מקבל את זמן המעבד
- מחשב מריץ יותר תוכנות מאשר מספר המעבדים שלו
- נדרשת חלוקת משאבי המעבד בין Processים



תפקידי מערכת ההפעלה

2. ניהול הזיכרון

- קובעת את הקצאת הזיכרון לכל Process
 - טוענת את ה-Process ל-RAM
 - מחלקת את ה-RAM בין כל ה-Processes שרצים
- שומרת על אבטחה ופעולה תקינה
 - כל Process עובד במסגרת הזיכרון שהוקצה לו
 - לדוגמה, Word לא יכול לכתוב לזיכרון שמוקצה ל-Chrome
- כתיבה למקום אסור בזיכרון – מטרה של האקרים

תפקידי מערכת ההפעלה

3. ניהול התקני החומרה

- מידע זורם ממקלדת, עכבר, כרטיס רשת וכו' העברת המידע מהם אל ה-Processים וחזרה דורשת ניהול וקביעת עדיפויות
- מניעת התנגשויות כאשר Processים שונים רוצים לגשת אל אותה חומרה (דיסק קשיח, כרטיס רשת וכו')



תפקידי מערכת ההפעלה

3. ניהול התקני החומרה

מה קורה כשאנחנו שומרים קובץ במחשב?



תפקידי מערכת ההפעלה

4. ניהול מערכת הקבצים



- דומה לתפקיד של ספרן בספריה
- צריכה לקבוע היכן לשמור כל קובץ
- צריכה לשמור על "קטלוג" שיאפשר מציאה קלה של כל קובץ
- צריכה לדעת איזה קבצים פתוחים ולמנוע בעיות (Process) כותב לקובץ שפתוח על ידי Process (אחר)

מה למדנו?

- איך עובד המעבד?
- אילו סוגי זכרון קיימים?
- מהם תפקידי מערכת ההפעלה?