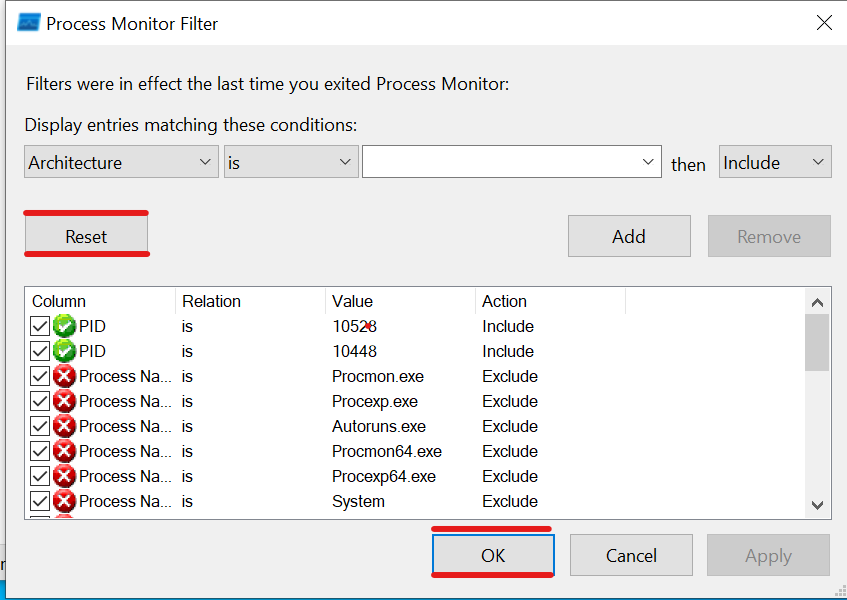
בס"ד

מערכות הפעלה – תרגיל 1

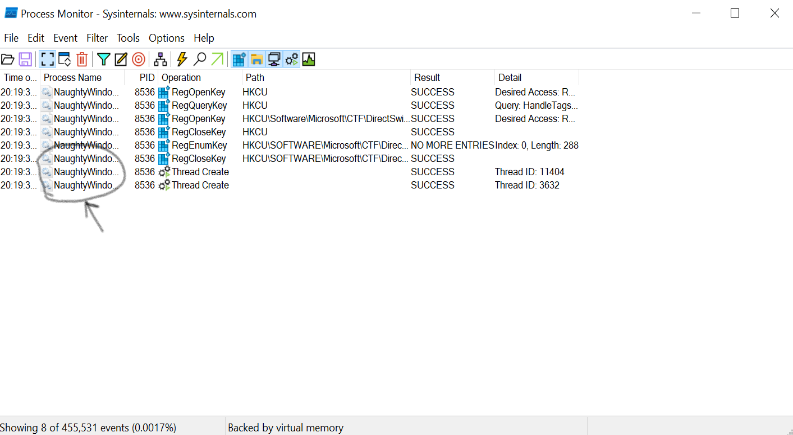
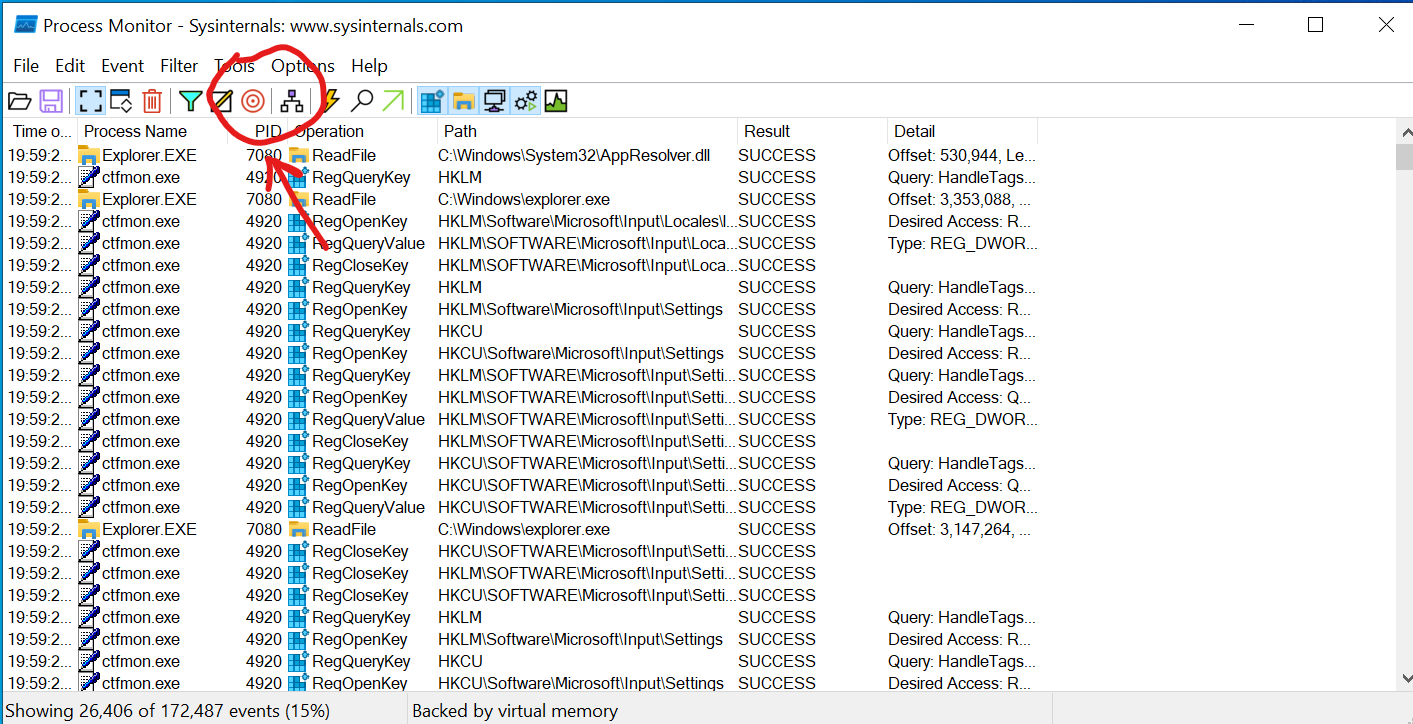
מדריך – כיצד להסיר את התוכנה הזדונית:

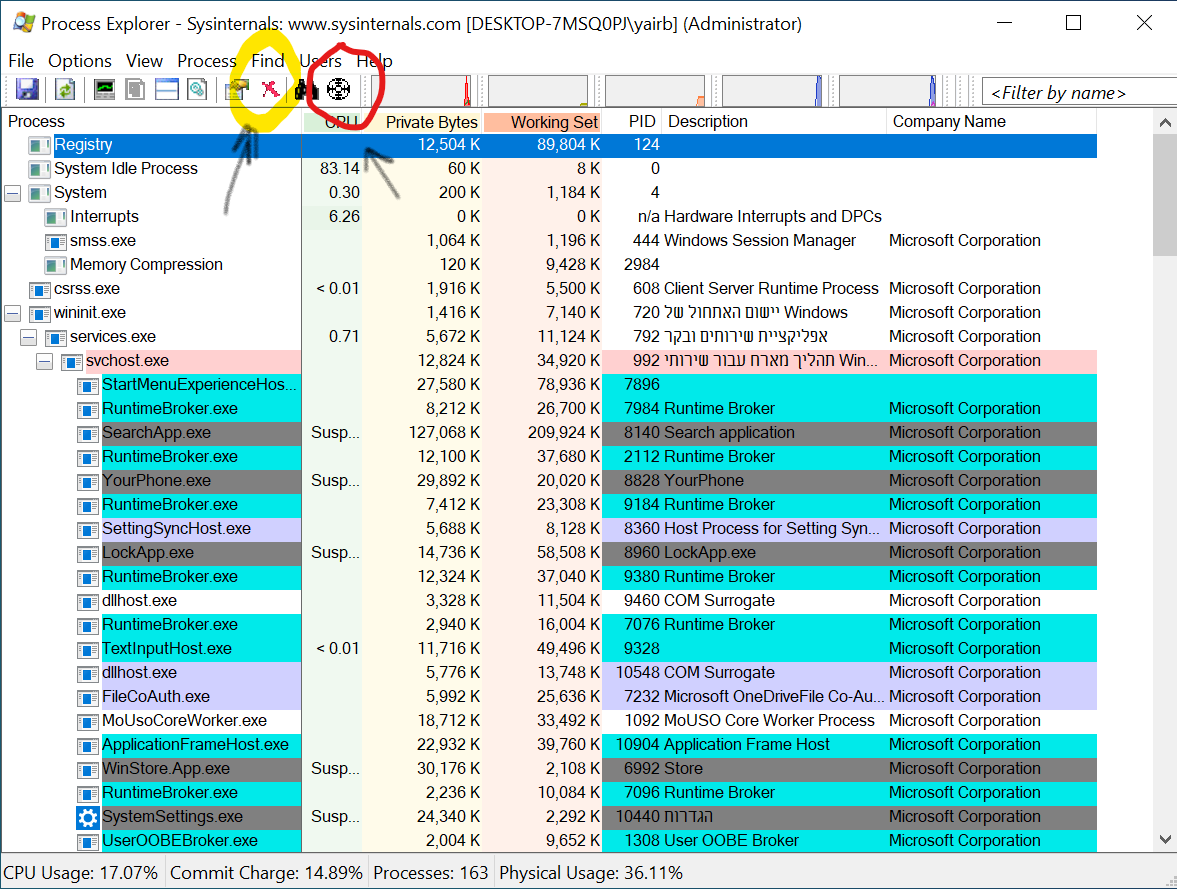
*הערה: המדריך יוצא מנק' הנחה שהורדת את קובץ הזיפ מהספר ואת התוכנה הזדונית*

1.פתח את ה- procmon לחץ על reset ולאחר מכן על .ok

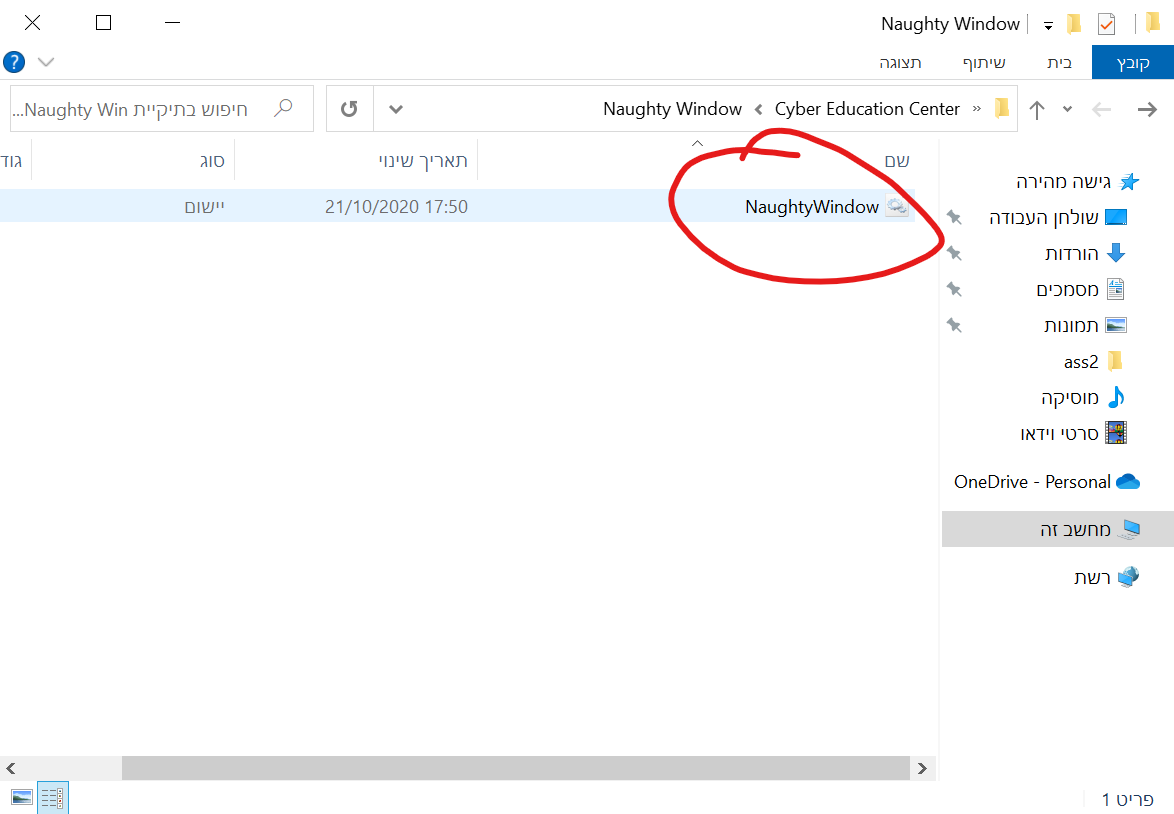


2.גרור את המטרה על החלונית ועמוד על **הפעולה** שתופיע כדי לראות היכן הקובץ מאוחסן – זכור את המקום כדי שתוכל למחוק את הקובץ משם

**

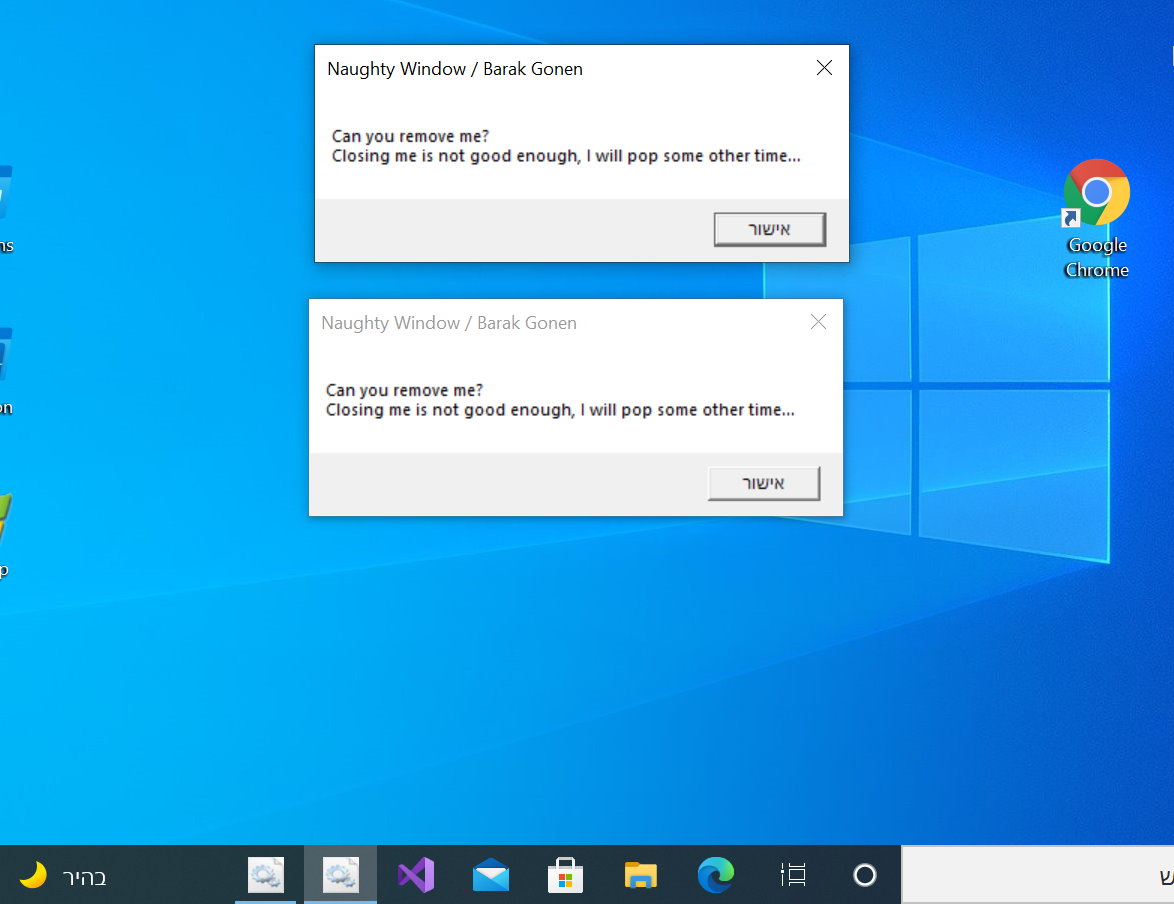
3.פתח process explorer גרור את **המטרה** על החלונית ולחץ על כפתור הkill**

4. כנס לסייר הקבצים למקום שבו מאוחסן הקובץ(מסעיף 2) ומחק אותו

**

5.הפעל מחדש את המחשב

6. לאחר הפעלת המחשב מחדש יקפצו לך 2 חלוניות שמפעילה התוכנית – עליך לבצע את הפעולות 1-5 על שתיהן וכך התוכנה תוסר.

**

תשובות לשאלות:

1. bootstart (הwinsafe רק מקפיץ אותו והקובץ הראשוני – נאטי ווינדווס שיקרי)
2. Bootstart.exe שמותקן ב C:\Windows \BootStart.exe –
3. הwinsafe מפעיל אוטומטית את הבוטסטארט בכל הפעלת מערכת ולכן זה חזר אחרי הריסטרט – הפרוססים הפועלים הם ווינסייפ ובוטסטארט ומיקומם ב C:\Windows \BootStart.exe וב C:\Windows \winsafe.exe