נכנסתי לprocmon עשיתי פילטר לפי שם וסוג פקודה שהיא משתמשת ואז ראיתי איזה פרוסס יש ואז נכנסתי לאותו פרוסס שהיה בו את הקובץ הרצה ואז הגעתי לתמונה למעלה