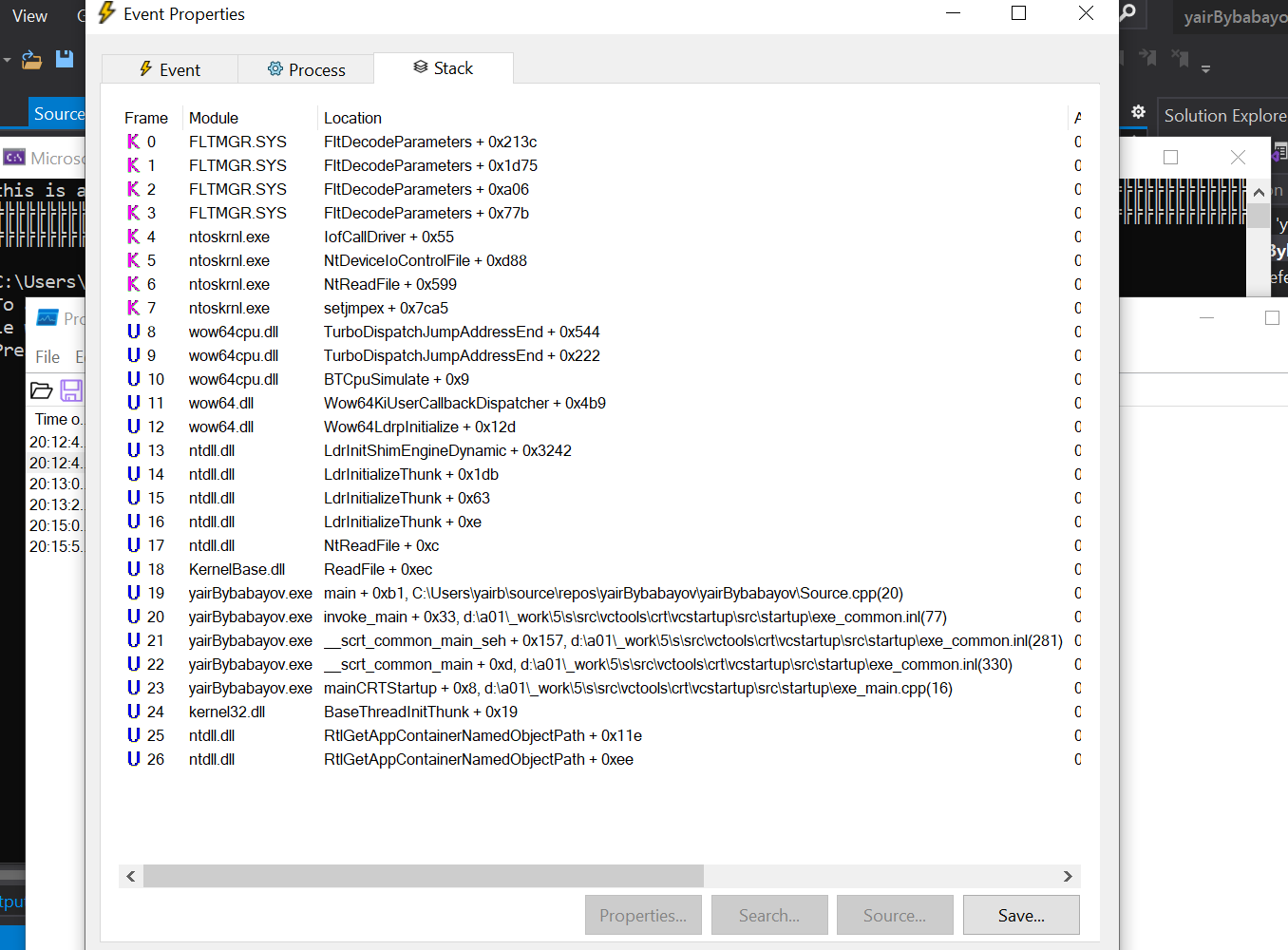
בס"ד

**מערכות הפעלה תרגיל 2**



הערה: המחסנית לא אמורה להכיל גם יוזר לנד וגם קרנל אלא זה משהו מיוחד שהפרוקמון עושה.

בשורה 21 התוכנית מריצה את הmain.

בשורה 19 – קורא לreadfilE

בשורה 18 בתוך הreadfile נכנס לקרנלבייס

בשורה 17 הreadfile נכנס לntdll

ממשיך בתוך הntdll עד שורה 12 ושם נכנס לwowdll

נכנס עוד עד שלבסוף בשורה 7 מגיע לתוך הkernel – (מהיוזר לנד)

לאחר שהוא נכנס לקרנל הוא יכול לגשת ולקרוא את המידע וזה מה שקורא בשורה 6

בשורה 3 ניתן לראות שהוא עושה DECODE ומפענח את הבינארי

כך עד שהוא מגיע ל0