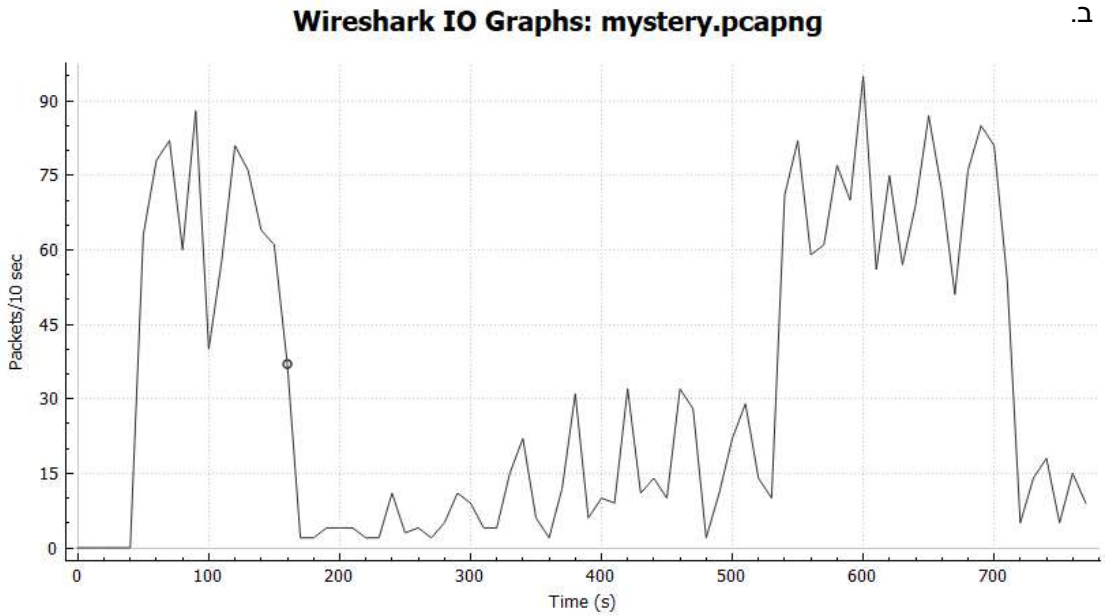
מגישים: 200878627 יניב לידן
204736961 דן אברהם

אבטחת מחשבים ורשתות תקשורת – עבודה 1 חלק א'

1. א. השתמשנו ב-display filter לפי כתובת ה-ip של המשתמש ושאורך ה-data גדול מ-1.
ip.addr==10.100.102.74&&data.len>0

ב.



ג. לפי ניתוח ויזואלי בלבד ניתן להניח כי הסשנים של הורדת הקבצים הם בהתחלה ובסוף(בשניות 40-160, 520-720 בערך), איפה שקצב העברת הנתונים הוא גבוה יותר. לעומת שאר הגרף שם קצב העברת הנתונים נמוך יחסית וכנראה שמדובר בסשנים של הגלישה באתרי אינטרנט.

2. א. בתפריט העליון תחת חלונית View באפשרויות של Name Resolution ניתן לסמן את Resolve Network Addresses והדבר יציג את כתובות האתרים.

ב. לחיצת היד הראשונה (הSYN וה-ACK הראשונים) עם אתר ONE היא לאחר 239.878895 שניות מרגע תחילת ההקלטה.

ג. לחיצת היד הראשונה (הSYN וה-ACK הראשונים) עם אתר YNET היא לאחר 377.145935 שניות מרגע תחילת ההקלטה.

ד. המשתמש ביקר בנוסף באתר www.quora.com.

ה.

	זמן התחלה (שניות מתחילת ההקלטה)	זמן סיום (שניות מתחילת ההקלטה)
הורדת וידאו ראשון	50.044284	171.851130
הורדת וידאו שני	536.864470	719.121810
גלישה ב-YNET	377.145935	477.037794
גלישה ב-ONE	239.878895	308.323388