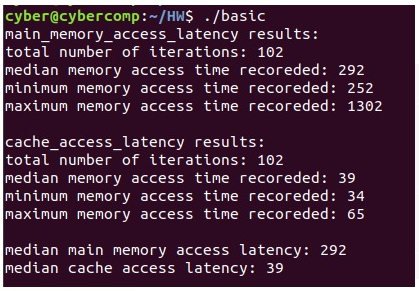
עקרונות וכלים באבטחת מחשבים - תרגיל בית 5

חן גולדנברג – 312141609

יואב כהן - 203115373

שאלות 1.1 + 1.2 :

מצורפת תמונה המכיל את תוצאת ריצה של שני האלגוריתמים (קבלת זמני גישה לזכרון הראשי וזמני גישה למטמון). בריצה זו דרשנו מינימום של 100 איטרציות עד להתייצבות החציון.  
 ע"מ לדייק את התוצאה אף יותר ניתן לבצע מספר איטרציות גדול בכמה סדרי גודל.



שאלה 1.3:

ניתן לבחור כל מספר הגיוני שמתאים להפרדת זמני הגישה לזכרון הראשי למטמון. ראינו בסעיפים קודמים שזמן הגישה הממוצע למטמון הוא בערך 39 מחזורי שעון, והגישה לזכרון הראשי היא בסביבות 292 מחזורי שעון.

לצורך בחירת ערך הסף אשר יבדיל האם הכתובת שאליה ניגשנו נמצאת במטמון או בזכרון הראשי, ניתן לבחור מספר שנמצא באמצע בין מקסימום מחזורים לגישה למטמון (65) למינימום מחזורים לגישה לזכרון הראשי (252).

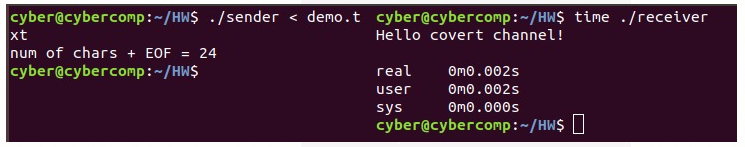
נקבל כי ערך הסף הנבחר הוא:

שאלה 1.5:

לצורך חישוב קצב התעבורה לביט נעזרנו בתוכנית לצורךף ספירת מספר התווים שעוברים והתקשל שכולל תו הEOF ישנם 24 תווים. כל תו הוא 8 ביט, ולכן סה"כ אנו מעבירים ביטים.

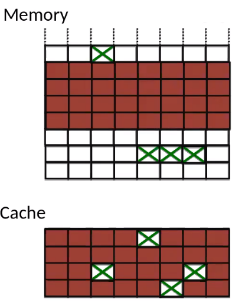
ניתן לקראות בתמונה המצורפת שזמן הריצה של התוכנית הוא 0.002 שניות.

ומתקבל קצב התעבורה הבא :



שאלה 2.1:

בקוד המצורף ניתן לראות שבמידה והMSB של תא מסויים במערך המידע מקיים שערכו הוא אפס – אנו ניכנס לתוך הIF בקוד, ובכך תוקף יכול להזליג את הביט הבודד הנ"ל בעזרת מתקפת תזמון המטמון. כלומר, עבור המערך הנתון, אשר בגודל 100 – דולפים 100 ביט.  
ובאופן כללי, למערך סודות בגודל n דולפים n ביטים.

שאלה 2.2:

תקיפת Prime and Probe

מודל התקיפה -

* התוקף והנתקף רצים מעל אותה ליבה. כלומר המשאב המשותף הוא מטמון 1L.
* התוקף בעל יכולות user space.
* התוקף מכיר את הקוד הנתקף, ואת המיפוי של כל שורה בקוד.

תיאור התקיפה -

* התוקף יוצר באפר שנשמר בזיכרון בגודל זיכרון המטמון.
* התוקף נכנס לכל הבאפר ובכך ממלא את המטמון במידע שלו.
* הקורבן מבצע את קטע הקוד שלו ובכך מפנה חלק מהבלוקים במטמון שהתוקף הכניס.
* התוקף שוב מבצע גישה לכל הבאפר ומודד את זמני הגישה עבור כל בלוק.

הסטים אליהם הקורבן ניגש הם אלו עבורם זמן הגישה גדול יותר.

* התוקף שומר העתק של גישות הנתקף וע"י הנדסה לאחור יכול לגלות את הMSBים בעזרת התבוננות בשורה המטמון שמכילה את .

שאלה 2.3:

נתאר את השינוי בקוד שימנע את התקיפה שתארנו בסעיף קודם תוך שמירה על נכונות הקוד:

נציע את שני הפתרונות המצורפים, כאשר המחשבה מאחוריי המימוש נובעת מהרצון לבטל את יכולת התוקף להשיג מידע אודות תוכן הסוד שמתקבל בעקבות מעקב על שורת המטמון המתאימה.

בשני הפתרונות המוצעים דאגנו לעדכן את תוכן המשתנה בכל ריצה של האיטרציה. תוכן ה משתנה בהתאם לערך הMSB, אך מאחר ואנו מעדכנים את ערכו בכל איטרציה – התוקף תמיד רואה שיש גישה לשורת המטמון ואינו יכול להסיק מידע על הMSB.

