**חלק 2**

**פתחו את wireshark( במידת הצורך - הורידו והתקינו את wireshark).**

**ביחרו את כרטיס הרשת שאתם גולשים דרכו והתחילו להסניף את המידע.**

**פתחו דפדפן וגלשו באינטרנט למספר אתרים.**

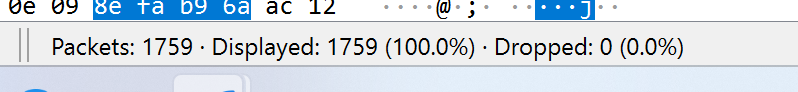
**עיצרו את הסנפת התעבורה.**

**א.**

**כמה חבילות הוסנפו? )הסתכלו בחלק התחתון של התוכנה** הוסנפו 1759 חבילות

A screenshot of a computer

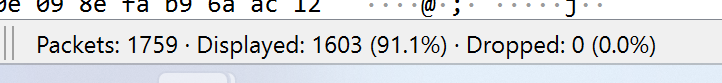
Description automatically generated



ב **בעזרת שורת הסינון, סננו רק חבילות שנשלחו על גבי פרוטוקול udp. כמה חבילות כאלה**

**יש?** יש 1603 חבילות בפרוטוקול UDP A screenshot of a computer

Description automatically generated



**ג. בידקו מהי כתובת ה IP במחשב שלכם שאתם משתמשים בה כרגע )למשל בעזרת**

**.)ipconfig/ifconfig**

הכתובת של המחשב שלנו: 172.18.59.186

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

**ד. מבין שלל החבילות שהסנפתם ביחרו חבילת DNS( תוכלו לזהות אותה לפי העמודה**

**Protocol). שימו לב, DNS הינו פרוטוקול שכבת אפליקציה, שרץ על גבי פרוטוקול udp**

**בשכבת התעבורה.**

**- האם החבילה נשלחה אל המחשב שלכם או שאתם שלחתם אותה מהמחשב שלכם?**

**הסבירו כיצד הגעתם למסקנה.**

**A screenshot of a computer

Description automatically generated**

זה צילום מסך כללי לסעיף ובשביל הדגשות, צילומים חלקי מסך

חבילה מספר 7, החבילה נשלחה מהמחשב שלנו, אנחנו שלחנו אותה.

A screen shot of a computer

Description automatically generated

ניתן להסיק זאת SRC IP ששווה ל 172.18.59.186 שזו בדיוק הכתובת IP שמצצאנו בסעיף קודם למחשב שלנו.



**- הסתכלו על פירוק החבילה לשכבות. מאיזה פורט נשלחה החבילה? לאיזה פורט נשלחה**

**החבילה? כלומר, לאיזה פורט האזין הלקוח ולאיזה פורט האזין השרת?**

החבילה נשלחה אל פורט 53, השרת האזין לפורט 53

ונשלחה מפורט 60694, הלקוח האזין לפורט 60694

A close up of a computer screen

Description automatically generated

**- הדגימו בתוך שכבת הרשת את כתובת ה IP של השולח ואת כתובת ה IP של המקבל.**

**שימו לב, במידה והחבילה שבחרתם אינה השתמשה ב 4IPv, ביחרו חבילה אחרת )אם**

**אתם לא רואים כתובת IP כמו שראינו בכיתה - אזי ביחרו חבילה אחרת(.**

**A screenshot of a computer

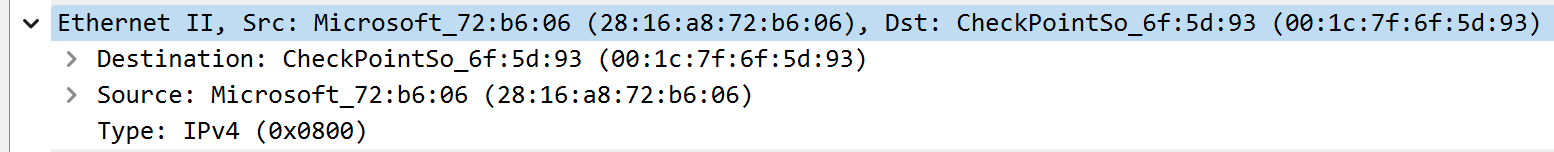
Description automatically generated**

גרסא 4, IPV4

IP שולח: 172.18.59.186

IP מקבל: 132.70.60.124

**- מהי כתובת ה MAC של השולח? ומהי של המקבל?**

****

כתובת MAC של השולח:

28:16:a8:72:b6:06

כתובת MAC של המקבל:

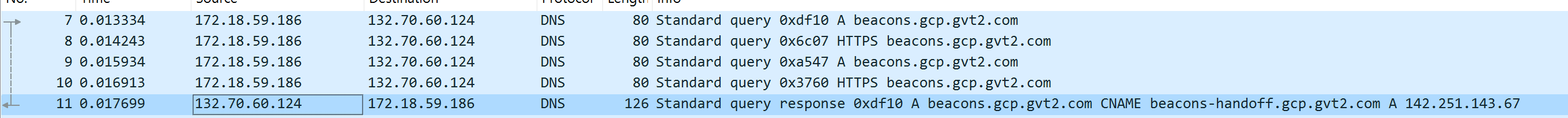
00:1c:7f:6f:5d:93

**ה. חיזרו על סעיף ד' - אך כעת עם החבילה ההפוכה. כלומר, אם בסעיף ד בחרתם בחבילה**

**שהמחשב שלכם שלח - כעת ביחרו את החבילה שהמחשב שלכם קיבל. שימו לב, עליכם לבחור**

**את החבילה הספציפית שמתאימה.**

החבילה הספציפית המתאימה היא לא אחרת מאשר: 11



החבילה נשלחה אל המחשב שלנו

ניתן להסיק זאת מsrc ip שניתן לראות שהוא 132.70.60.124 שזוהי כתובת הIP לא שלנו, וכן הDST IP היא בדיוק הכתובת של המחשב שענינו בג.

A screenshot of a computer

Description automatically generated



החבילה נשלחה מפורט אליו מאזין השרת – 53, ונשלחה אל הפורט אליו מאזין הלקוח -60694



הדגמת כתובות הIP.

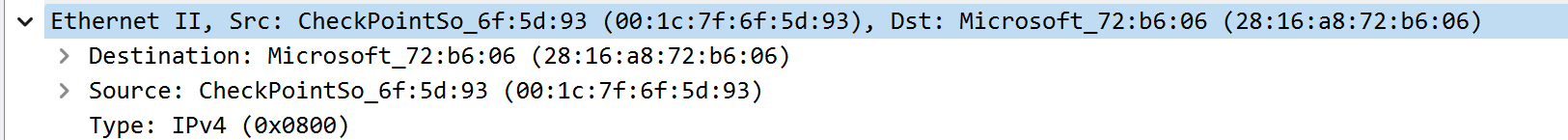
A screenshot of a computer

Description automatically generated

כתובת MAC של המקבל:

28:16:a8:72:b6:06

כתובת MAC של השולח:

00:1c:7f:6f:5d:93

**ו. בעזרת שורת הסינון, סננו את כל החבילות כך שיופיעו רק חבילות שהמחשב שלכם שלח ורק**

**חבילות בפרוטוקול DNS. הסתכלו על שכבת התעבורה של כמה מהחבילות - ובפרט על ה**

**port source שלהם וה port destination שלהם. האם אתם שמים לב למשהו? מה**

**המשמעות של זה?**

**A screenshot of a computer

Description automatically generated**

בכולן הdst פורט הוא 53, הSRC פורט משתנה בין החבילות

המשמעות היא שכל החבילות שהמחשב שלנו שולח נשלחות ומתקבלות באותו פורט (הפורט שהשרת מאזין אליו)

A screenshot of a computer

Description automatically generated**A screenshot of a computer

Description automatically generated**

חבילות שהסתכלנו בהן...

**ו. בעזרת שורת הסינון, סננו את כל החבילות כך שיופיעו רק חבילות שהמחשב שלכם קיבל ורק**

**חבילות בפרוטוקול DNS. הסתכלו על שכבת התעבורה של כמה מהחבילות - ובפרט על ה**

**port source שלהם וה port destination שלהם. האם אתם שמים לב למשהו?**

**התשובה כאן אמורה להשלים/לחזק את תשובתכם לסעיף הקודם.**

**A screenshot of a computer

Description automatically generated**

עכשיו נשים לב שזה בדיוק הפוך, כל הSRC פורט זהים = 53, הDST שונים בין החבילות השונות

בעצם כל החבילות שהמחשב שלי מקבל נשלחות מאותו מקור (השרת)

A screenshot of a computer

Description automatically generated

חבילה שבדקנו כדי לראות את התכונה החוזרת, SRC PORT =53

**ז.**

**על בסיס תשובותיכם לשני הסעיפים האחרונים - כיצד תוכלו לבצע סינון בשורת הסינון לכל**

**החבילות שנשלחו בפרוטוקול DNS, בלי לסנן מפורשות לפי DNS( ?כלומר, אסור לכתוב dns**

**בשורת הסינון(**

נוכל לסנן ע"י מספר פורט (53)

ויציג לנו את כל החבילות שנשלחו בפרוטוקול DNS (החבילות שהפורט יעד שלהן הוא 53, אלו החבילות שהמחשב שלנו שלח לשרת, ואלה שהפורט מקור הוא 53 אלו הן החבילות שאנחנו קיבלנו מהשרת)

**A screenshot of a computer

Description automatically generated**