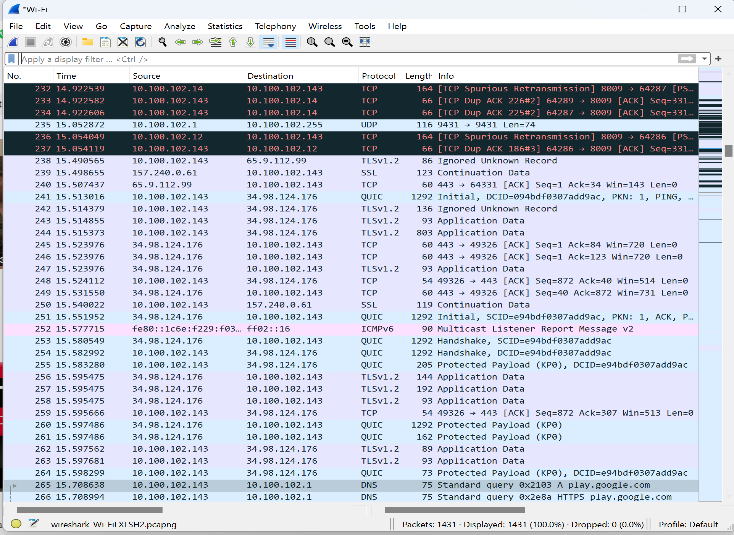
**חלק 2**

**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.**

1. **כמה חבילות הוסנפו? )הסתכלו בחלק התחתון של התוכנה(**

הסנפנו 1431 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 1117 חבילות בפרוטוקול UDP

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

**.)ipconfig/ifconfig**

כתובת הIP של המחשב שלנו היא:

10.100.102.143

**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.**

חבילה מספר 265, החבילה נשלחה מהמחשב שלנו, אנחנו שלחנו אותה.

ניתן להסיק זאת מsrc ip שניתן לראות שהוא 10.100.102.143 שבסעיף קודם הראנו וכתבנו שזוהי הכתובת IP של המחשב שלנו

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

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

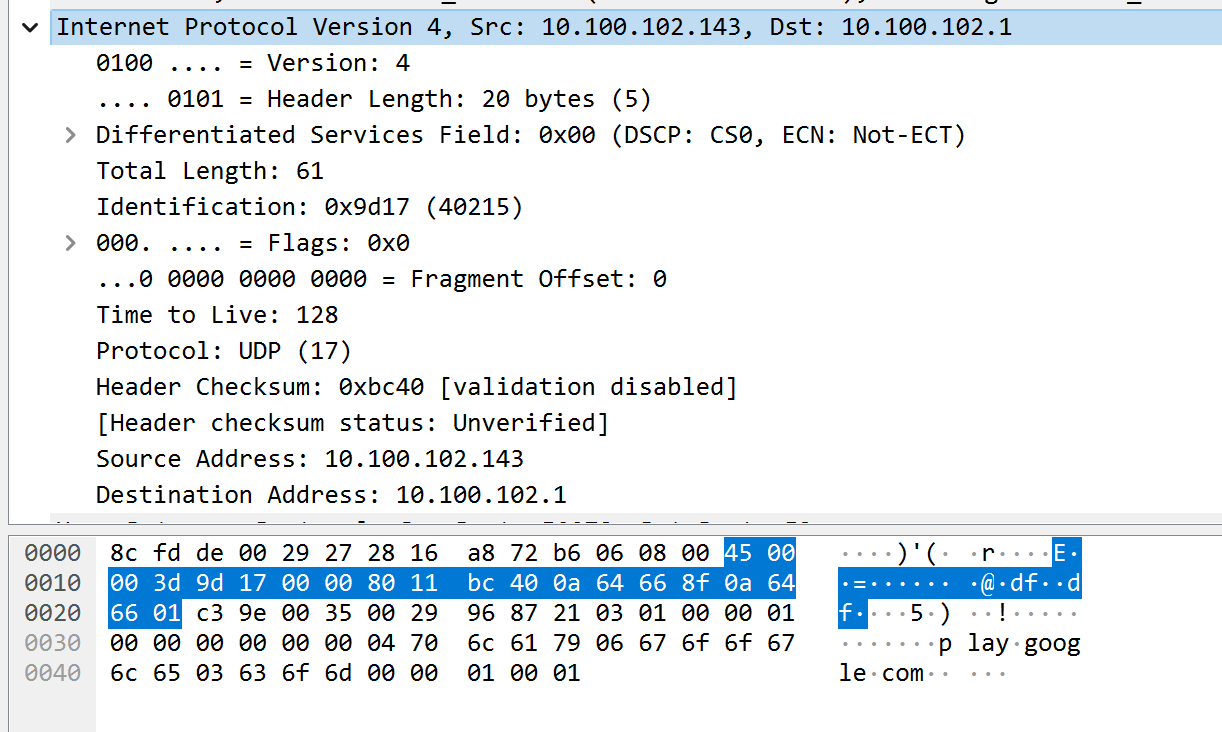
החבילה נשלחה מפורט 50078, הלקוח האזין לפורט 50078

ונשלחה אל פורט 53, השרת האזין לפורט 53

**- 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(.**

****

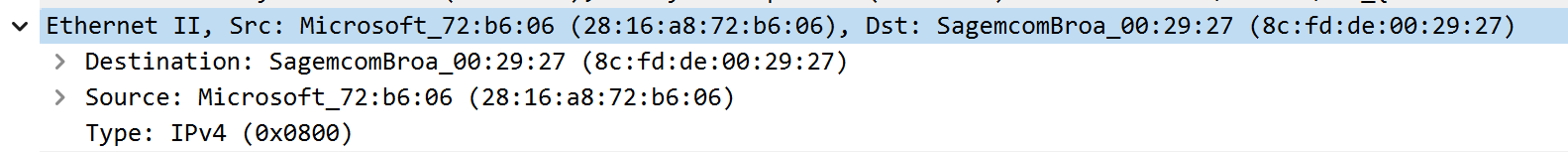
**- מהי כתובת ה MAC של השולח? ומהי של המקבל?**

כתובת MAC של השולח:

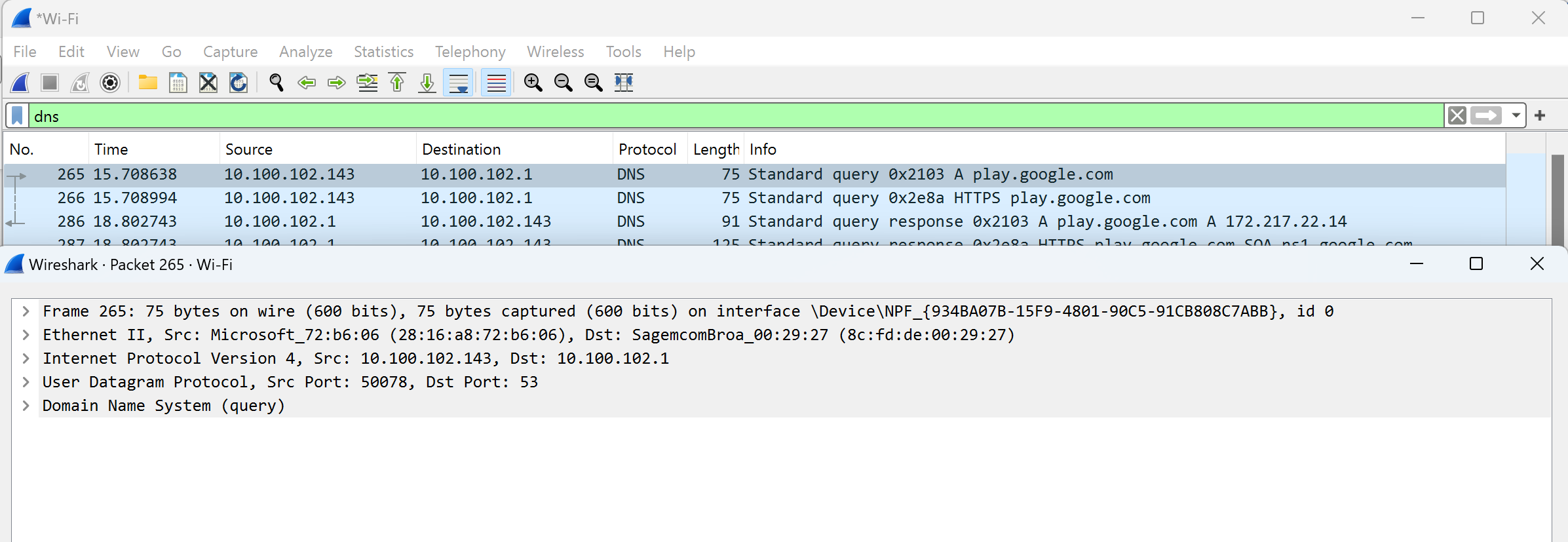
28:16:a8:72:b6:06

כתובת MAC של המקבל:

8c:fd:de:00:29:27



**צילום מסך לסעיפי ד:**

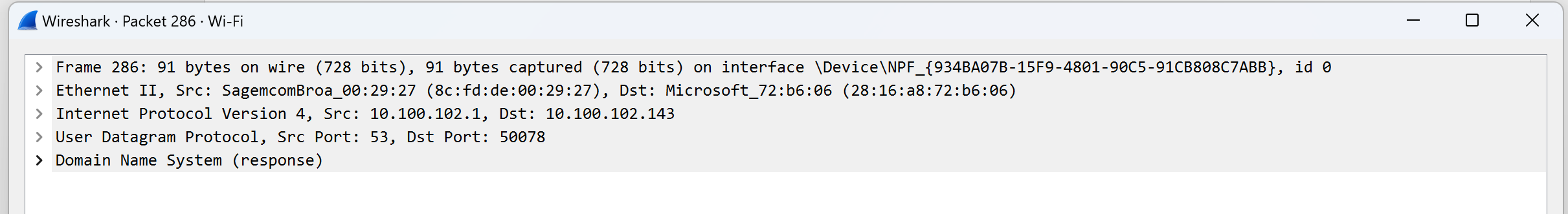
****

**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: 286



החבילה נשלחה אל המחשב שלנו

ניתן להסיק זאת מsrc ip שניתן לראות שהוא 10.100.102.1 שזוהי כתובת הIP לא שלנו, וכן הDST IP היא בדיוק הכתובת של המחשב שענינו בג.

החבילה נשלחה מפורט אליו מאזין השרת – 53, ונשלחה אל הפורט אליו מאזין הלקוח -50078

A screenshot of a computer

Description automatically generated

הדגמת כתובות הIP.

כתובת MAC של המקבל:

28:16:a8:72:b6:06

כתובת MAC של השולח:

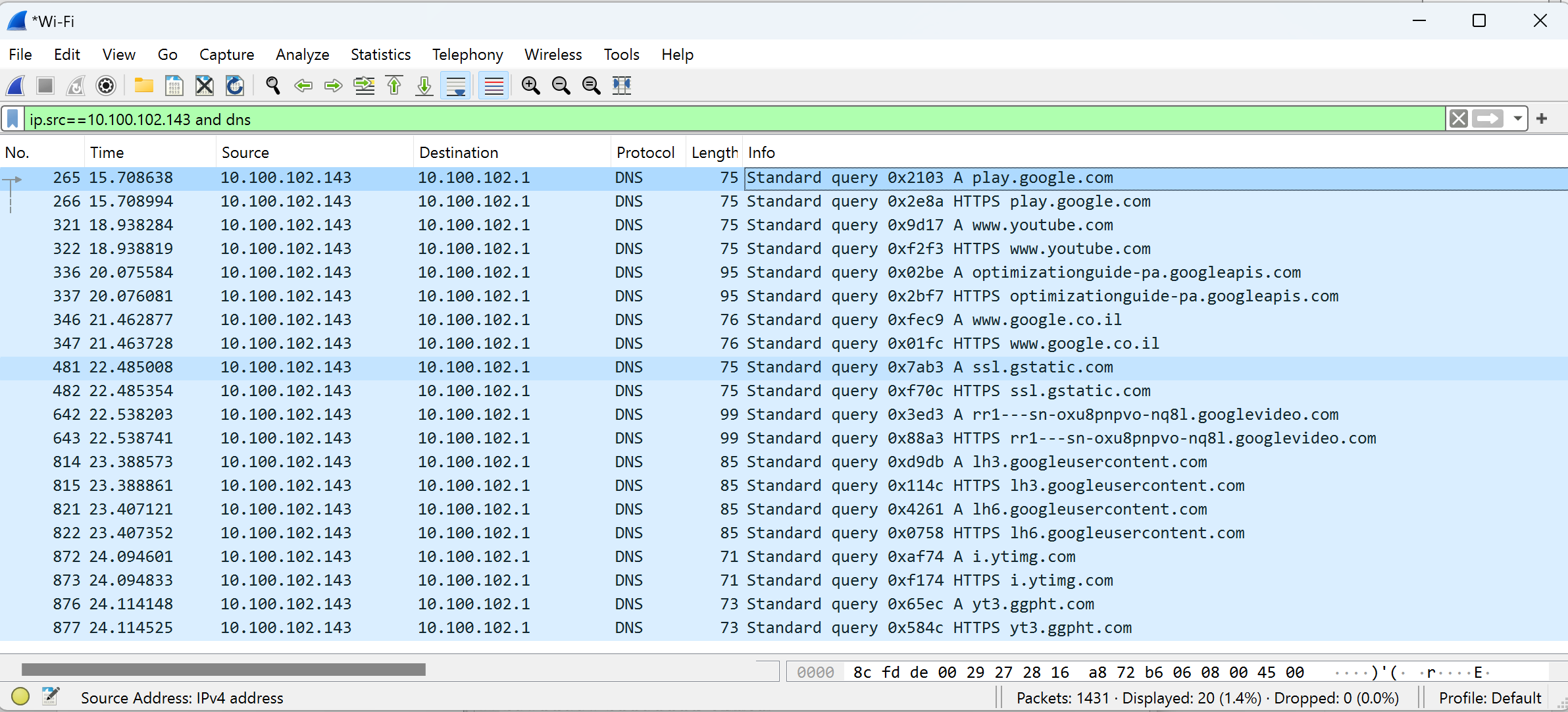
8c:fd:de:00:29:27

**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?**

****

בכולן הdst פורט הוא 53, הSRC פורט משתנה בין החבילות

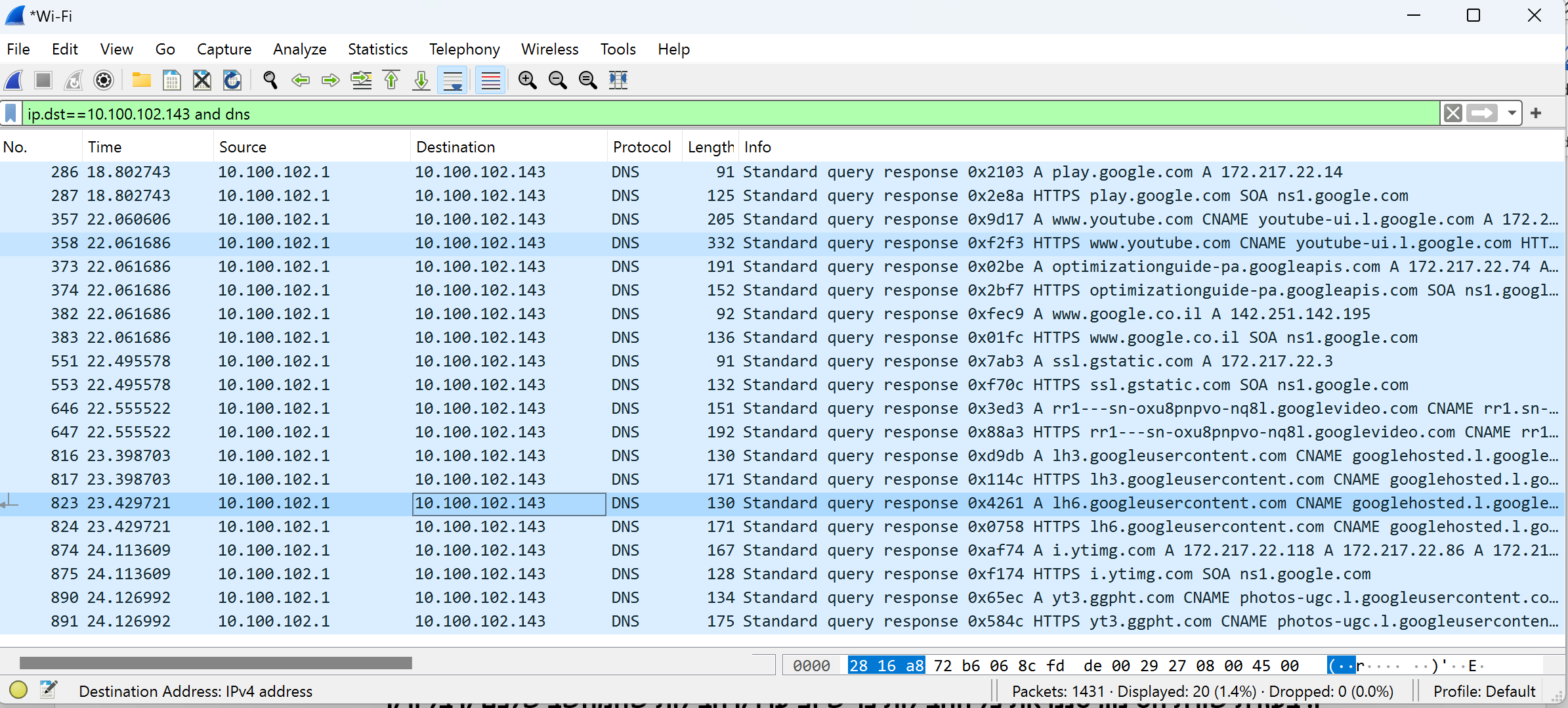
המשמעות היא שכל החבילות שהמחשב שלנו שולח נשלחות ומתקבלות באותו פורט

**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.**

****

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 כנראה)

**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)

אם נסנן עפ"י פורט יעד = 53 נקבל את כל החבילות DNS שהמחשב שולח

ואם עפ"י פורט מקור = 53, נקבל את כל החבילות DNS שנשלחות אל המחשב שלנו