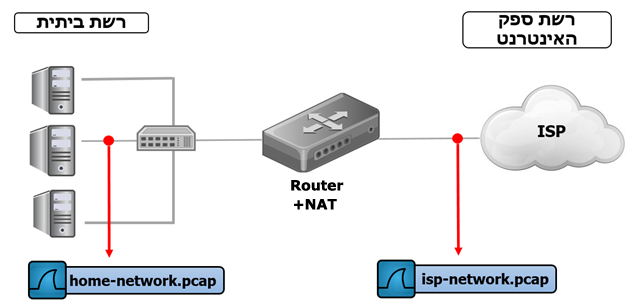
שיעור 11 – איך בונים רשת

**תרגיל: מעבדת NAT**

בתרגיל זה נכיר את פעולתו של רכיב ה-NAT מבפנים, בעזרת שתי הסנפות שנקבל ממקומות שונים ברשת.

**1. תמונת הרשת**

1. גלית פרשה כבלים, הקימה רשת ביתית והתחברה לספק האינטרנט "אינטרנט זהב".
2. גלית גלשה לאתר גוגל הנמצא בכתובת ה-IP: **64.233.169.104.**
3. בעזרת גמדי-רשת קטנים ושקופים, הוסנפה התעבורה בו זמנית בשני מקומות שונים ברשת, כפי שמסומן בתרשים הבא:

**2. חלק א' – ההסנפה ברשת הביתית**

1. פתחו את קובץ ההסנפה home-network.pcap בתוכנת Wireshark.
2. מהי כתובת ה-IP של גלית ברשת הביתית?

|  |
| --- |
| 192.168.1.1 |
| תשובה |

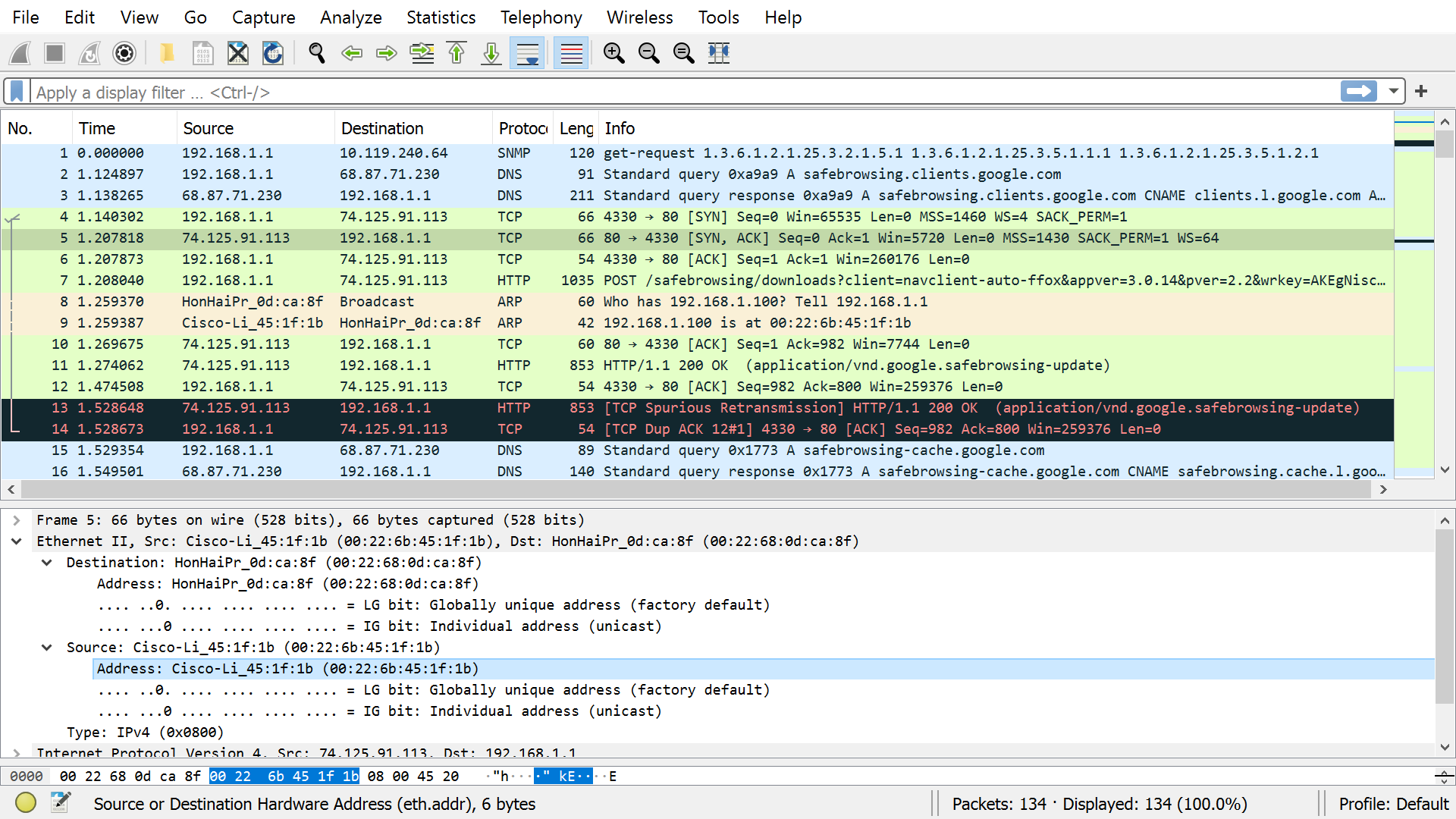
1. מהי כתובת ה-MAC של גלית?

|  |
| --- |
| 00:22:68:0d:ca:8f |
| תשובה |

1. האם אפשר לדעת ע"פ ההסנפות האם יש רכיב Switch ברשת של גלית? אם כן, כיצד? אם לא, מדוע?

|  |
| --- |
| לא כי לסוויטצ' אין IP או MAC הוא ישות בלתי נראית |
| תשובה |

1. מהו ה-IP וה-MAC של ה-NAT של גלית? כתבו כיצד מצאתם את המידע וצרפו צילומי מסך רלוונטיים.

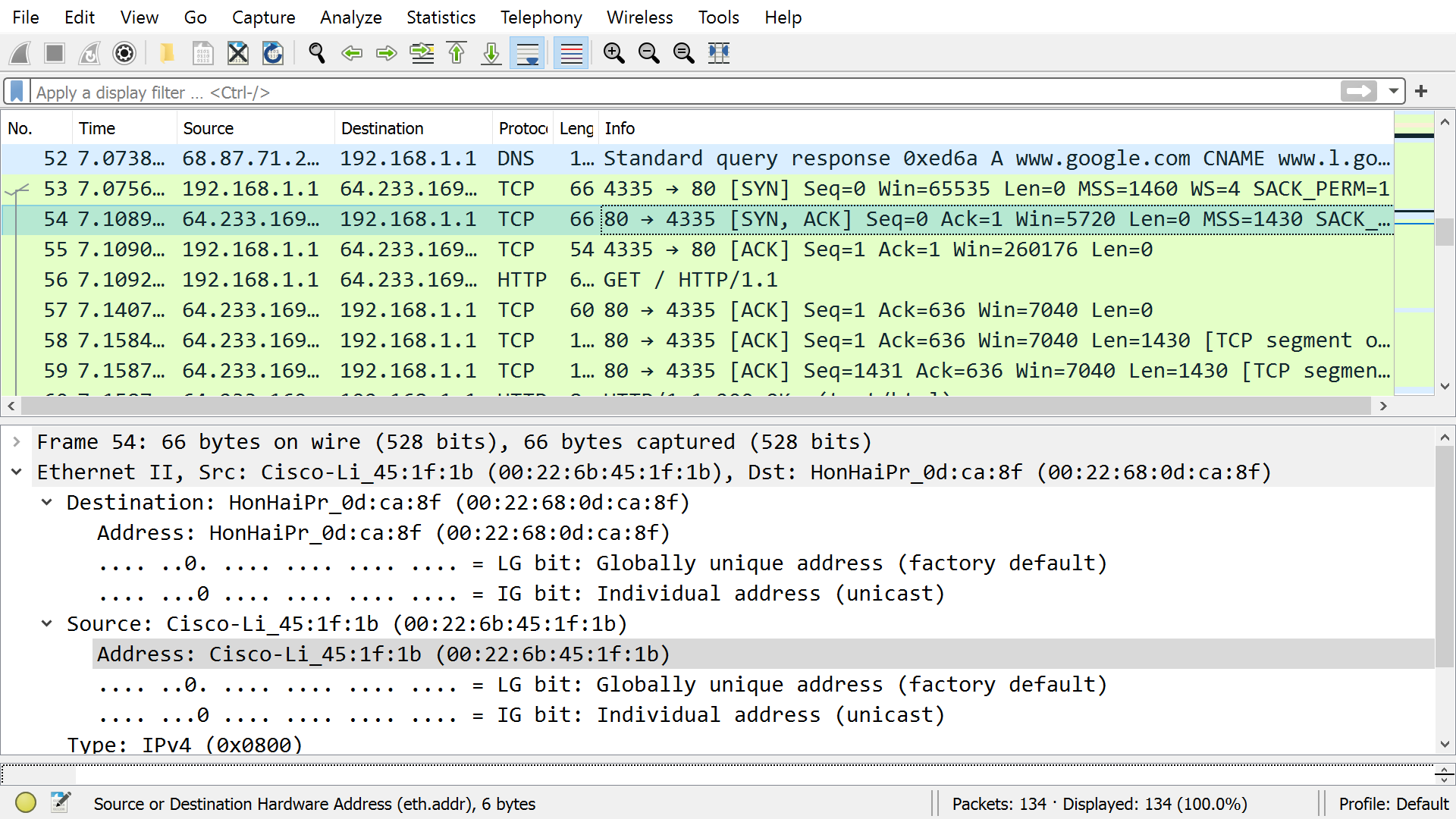


|  |
| --- |
| 192.168.1.100, 00:22:6b:45:1f:1b, גיליתי את המאק כשמגיעות אלינו חבילות ממחוץ לרשת הן חייבות לעבור דרך הNAT, לכן הMAC האחרון הוא של הNAT, ואז השוותי את הMAC לMAC שעונה לנו על הARP, וזה אותו MAC, ככה אני יודע את הIP. |
| תשובה |

1. הציגו את כל הגלישה של גלית לאתר גוגל. כתבו פה את הפילטר שכתבתם / הפעולות שביצעתם:

|  |
| --- |
| http && frame contains [www.google.com](http://www.google.com), או http && frame contains "google.com" אם רוצים גם את הדברים לפני שהם של גוגל אבל לא האתר גוגל.קום |
| תשובה |

1. מצאו את לחיצת היד המשולשת של גלית עם אתר גוגל וצרפו צילום שלה.  
   זכרו! כדי לראות את כל תעבורת TCP בשיחה ספציפית השתמשו ב-Follow TCP Stream.



1. מהם ארבעת המאפיינים של ה-Socket בצד הלקוח (גלית)?

|  |
| --- |
| Src IP = 192.168.1.1 Src Port = 4335  Dst IP = 64.233.169.104 Dst Port = 80 |
| תשובה |

1. מי היה היעד המיידי (ה-Next Hop) אליו שלחה גלית את החבילות שיועדו בסופו של דבר לגוגל? כיצד גיליתם זאת?

|  |
| --- |
| אל הNAT, כי בכתובת מאק של הדסטניישן בחבילות מגלית לגוגל כתוב את הכתובת של הNAT |
| תשובה |

**3. חלק ב' – ההסנפה ברשת ספק האינטרנט**

1. פתחו את קובץ ההסנפהisp-network.pcap .
2. אתרו את אותה שיחת HTTP שדנו בה בסעיף הקודם. האם יש הבדלים במאפייני ה-Socket שכתבתם בסעיף 2-ו'? אם כן, הסבירו מהם ומדוע קיים שוני?

|  |
| --- |
| כן, כי הכתובת SRC IP השתנתה משל גלית לשל הNAT של גלית, כי לא אכפת לאינטרנט הגדול איזה כתובת פרטית שלחה את החבילה אלא איזה כתובת ציבורית, הכתובת הפרטית תשמר בNAT כדי להעביר את התגובה למחשב הנכון |
| תשובה |

1. מהן שתי כתובות ה-IP שמחזיק ה-NAT שברשת הביתית? מהן שתי כתובות ה-MAC שלו?

|  |
| --- |
| 192.168.1.100 ו 71.192.34.104. הMAC הן אותו הדבר, כי MAC זה לפי כרטיס רשת פיזי, זה לא דינמי בכלל, לכרטיס אחד יש MAC אחד- לתמיד והכתובת היא-00:22:6b:45:1f:1c |
| תשובה |

1. כפי שלמדנו, רכיב NAT מחזיק בטבלה אשר מאפשרת לו לזהות שיחות שונות שעברו דרכו. מלאו את הטבלה בהתאם להסנפה שלנו:

**הערת החניך: השאלה הזאת לא ממש ברורה- צריך להתחיל מהDNS?, מהHTTP? להתחיל מתחילת הHTTP או הבקשת גוגל.קום? לעשות לגמרי את הכל ולהוסיף שורות??? או למלא רק את הזאת שנתנו לנו??? זה הכללי אז אם כתבתי שטויות, תתחשב בבקשה🙏**

|  |  |
| --- | --- |
| **טבלת NAT** | |
| **כתובת חיצונית + פורט** | **כתובת פנימית + פורט** |
| 53, 68.87.71.230 (DNS) | 51554, 192.168.1.1 (DNS) |
| 80, 74.125.91.113 (TCP SYN HTTP) | 4330, 192.168.1.1 (TCP SYN HTTP) |
| 80, 74.125.106.31 | 4331, 192.168.1.1 |
| אם צריך להוסיף שורות- אז אין לי כוח לעשות הכל אוביסלי | כי זה איזה מאתיים או משהו, קיצר עשיתי את זה ואני עושה עוד אחד וזהו |
| 80, 64.233.169.104 | 4335, 192.168.1.1 |

1. האם ה-NAT מבצע החלפת פורטים? הסבירו כיצד אתם יודעים זאת.

|  |
| --- |
| לא, כי הפורט לשרת הוא כנראה סטטי כמו 80 אז אין למה לשנות אותו והלקוח, הפורט שהוא שולח לך הוא הזה שהוא מקשיב בו, לכן אם תשנה אותו הלקוח לא יקבל את החבילה. חוץ מכל זה השוויתי את הפורטים בין הHOME לISP והם אותו הדבר... |
| תשובה |

1. בשתי ההסנפות, סמנו את בקשת ה-GET הראשונה ששלחה גלית בשיחה עם גוגל (זו השורה עם שדה ה-Length שהוא 689). במסך השכבות של Wireshark, הרחיבו בעזרת כפתור הפלוס את שכבת התעבורה (TCP) כך שיוצגו כל הפרטים. האם אתם מזהים הבדלים כלשהם בשדות ה-TCP בין שתי ההסנפות? כיצד תסבירו זאת?

|  |
| --- |
| לא, אני עברתי שורה שורה ולא ראיתי אף הבדל, אני מסביר זאת ש-למה שכן יהיה הבדל... השכבה חושבת שהיא היחידה, היא לא שמה לב בין קפיצות ממש, רק להגיע מA לB סוג של... (אני ממש מרגיש כאילו התשובה הייתה אמורה להיות כן אבל אני לא מוצא אף הבדל...) |
| תשובה |

1. עשו אותו דבר בשכבת הרשת (IP). האם אתם מזהים הבדלים בין שתי ההסנפות? כיצד תסבירו זאת?

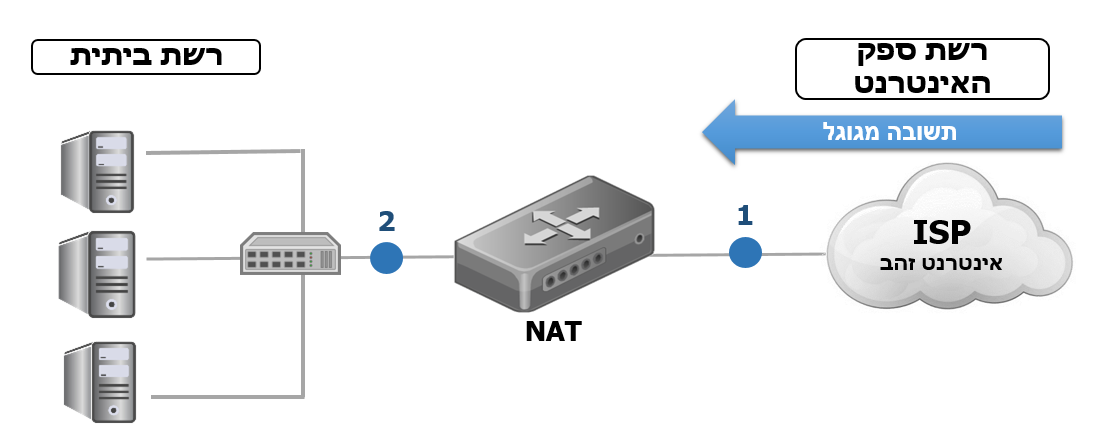
|  |
| --- |
| כן, יש בצ'קסאם, בטיים טו ליב (שזה הגיוני כי זה קפיצה אחת פחות), וכמובן בכתובת IP SRC כי יש את ההבדל של IP ציבורי ופרטי...  ההסבר הוא שוב שהIP הפרטי לא יעזור לאינטרנט הגדול, יש מיליוני אייפים כאלה במיליוני רשתות פרטיות, אז האייפי הופך להיות הIP של הנתב |
| תשובה |

1. **בונוס:** קראו באינטרנט כיצד מחושב שדה ה-Checksum של TCP. הסבירו מדוע הוא משתנה למרות שאף שדה בסגמנט TCP לא השתנה?

|  |
| --- |
|  |
| תשובה |

המשך לתרגיל בדף הבא....

**3. חלק ג' – תשובה חוזרת מגוגל**

1. התשובה חזרה מגוגל. בתרשים מתוארות שתי נקודות בהן עצרנו את החבילה החוזרת מגוגל. ענו על השאלת הבאות:
2. עבור החבילה בנקודה 1 המסומנת בתרשים, מלאו את הפרטים הבאים:

|  |
| --- |
| Src IP = 64.233.169.104  Dst IP = 71.192.34.104 Dst MAC = 00:22:6b:45:1f:1c |
| תשובה |

1. עבור החבילה בנקודה 2 המסומנת בתרשים, מלאו את הפרטים הבאים:

|  |
| --- |
| Src IP = 64.233.169.104 Src MAC = 00:22:6b:45:1f:1b  Dst IP = 192.168.1.1 Dst MAC = 00:22:68:0d:ca:8f |
| תשובה |