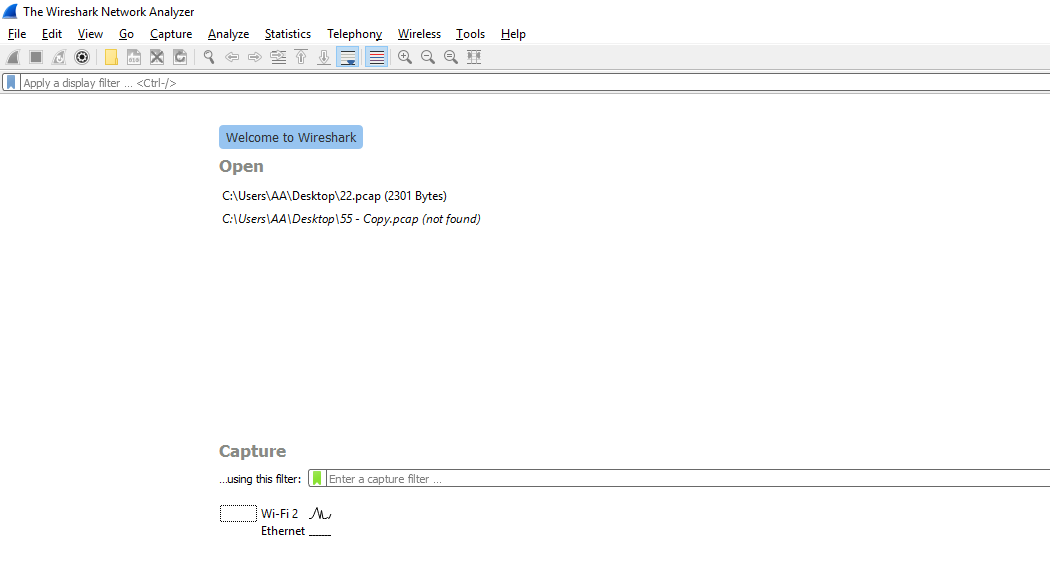
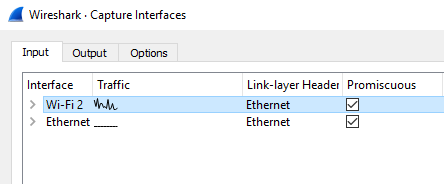
שיעור 4 – מודל השכבות והיכרות עם Wireshark

**תרגיל: היכרות עם Wireshark**

בתרגיל זה נתרגל הסנפה ראשונה עם תוכנת Wireshark. במהלך התרגיל נשתמש בתכונות החשובות של התוכנה עליהם למדנו בשיעור – החלוניות השונות של התוכנה ושימוש בשדה הפילטר.

**1. התחלת הסנפה**

1. פתחו את תוכנת Wireshark.
2. תחת הכותרת Capture מופיעים הממשקים הקיימים במחשב (לרוב יהיה לנו פה Wi-Fi וחיבור כבל – Ethernet).
3. ליד כל ממשק יש גרף המציג את הפעילות שלו בלייב.
4. בדקו מהו הממשק הפעיל ביותר על פי הגרף, לחצו עליו פעמיים וההסנפה תתחיל.



1. אם כל הזמן מתווספות שורות (חבילות) בחלק העליון, סימן שההסנפה עובדת כמו שצריך.

**2. היכרות עם המידע בחלון העליון**

1. חפשו את עמודת הזמן (Time) אשר מודדת את הזמן מאז תחילת ההסנפה בשניות. בעזרת עמודת המספור (No.), נסו לספור כמה חבילות נלכדו בשנייה אחת של הסנפה, וכמה חבילות נלכדו ב-10 שניות.

|  |
| --- |
| 183 |
| תשובה |

1. התבוננו בעמודות של כתובת IP מקור (Source) ויעד (Destination). נסו להבין מהי כתובת ה-IP של המחשב שלכם (מבלי להיעזר ב-ipconfig).

|  |
| --- |
| 10.100.102.99 |
| תשובה |

1. כתבו לפחות חמישה פרוטוקולים שונים שמצאתם בהסנפה.

|  |
| --- |
| Udp http dns tlsv1 tcp |
| תשובה |

**3. ביצוע סינונים (Filter)**

1. עצרו את ההסנפה בעזרת מקש ה-Stop האדום. בעזרת השורה התחתונה ביותר בתוכנה, כתבו כמה חבילות סה"כ נלכדו.

|  |
| --- |
| 8608 |
| תשובה |

1. כתבו סינון שיציג רק חבילות בפרוטוקול **HTTP**. כמה חבילות בפרוטוקול זה נלכדו?

|  |
| --- |
| 2 |
| תשובה |

1. כתבו סינון שיציג רק חבילות **שיצאו** מה-IP של מחשבכם. כתבו את שורת הסינון פה:

|  |
| --- |
| ip.src == 10.100.102.99 |
| תשובה |

1. כתבו סינון שיציג רק **חבילות HTTP שנכנסו אל ה-IP של מחשבכם.** כתבו את שורת הסינון:

|  |
| --- |
| ip.dst == 10.100.102.99 |
| תשובה |

**4. חיפוש מידע בהסנפה**

1. התחילו הסנפה חדשה, והיכנסו לאתר **groopy.co.il**.
2. נסו לבצע התחברות (login) באתר עם שם משתמש **magshim999** וסיסמא **123123**.
3. בדקו מהו ה-IP של האתר groopy.co.il כפי שלמדנו בשיעור הראשון.
4. בצעו סינון (Filter) ב-Wireshark כך שתראו רק את החבילות היוצאות / הנכנסות ל-IP של האתר. כתבו את שורת הסינון:

|  |
| --- |
| ip.addr == 192.114.70.79 |
| תשובה |

1. האם ניתן לראות בהסנפה את שם המשתמש והסיסמא? נסו למצוא אותם באחת החבילות שנשלחו לאתר. (שימו לב לחלון התחתון ביותר של Wireshark). צרפו צילום מסך של השם והסיסמא:  
   