

כבלכריש

בתרגיל זה נתנסה בשימוש בכלי Wireshark. נבצע מחקר קובץ הסנפה שהתקבל בעקבות גלישה

לאתר אינטרנט.

1. מצאו חבילה בפרוטוקול DHCP. מה כתובת ה IP  של היעד? באיזה פילטר השתמשתם?

|  |
| --- |
|  |

255.255.255.255  
dhcp

1. האם יש עוד חבילות שיש להם כתובת יעד IP  זהה.

|  |
| --- |
|  |

לא

החל מנקודה זאת, התעלמו מחבילות **שמספרן הסידורי קטן מ 17**.

1. במהלך ההסנפה בוצעה גלישה לאתר כלשהו. באיזה פילטר תשתמשו כדי למצוא את החבילות הללו?

|  |
| --- |
|  |

http

1. מצאו לאיזה אתר בוצעה הגלישה.

|  |
| --- |
|  |

www.themarker.com

1. מהי כתובת ה IP של האתר אליו בוצעה הגלישה?

|  |
| --- |
|  |

104.71.205.112

1. מהו הפורט אליו בוצעה הגלישה?

|  |
| --- |
|  |

80

1. מהו הפורט של הלקוח? (שימו לב יש מספר פורטים, עליכם למצוא את הראשון ממנו בוצעה גלישה לאתר)

|  |
| --- |
|  |

57311

1. מצאו חבילת http ששדה ה content-length שלה שווה בדיוק ל 14251 בתים.

Content-Length: 14251  
מצאנו חבילה מספר 119

|  |
| --- |
|  |

1. מתי נשלחה החבילה הראשונה ומתי נשלחה החבילה האחרונה עבור הפורט שמצאתם בסעיף 7?

|  |
| --- |
|  |

14.288893  
42.816510

1. תארו את דרך הפעולה שלכם על מנת לענות על שאלה 9?

|  |
| --- |
|  |

עשינו סינון לפי הפורט שמצאנו בשאלה 7 – 57311  
לאחר הסינון הסתכלנו על עמודת הזמנים ורשמנו את הזמנים של החבילה הראשונה בסינון ושל האחרונה.