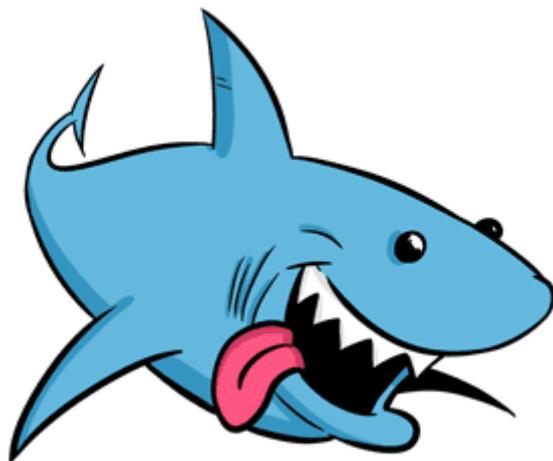


## כבלכריש



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

הורידו את קובץ ההסנפה מהלינק הבא:

[http://www.cyber.org.il/networks/basic\\_sniffing.pcapng](http://www.cyber.org.il/networks/basic_sniffing.pcapng)

וענו על השאלות הבאות:

1. מיצאו פקטה בפרוטוקול DHCP. מה כתובת ה-IP של היעד שלה? (זוהי כתובת IP מיוחדת ונלמד עליה בבוא הזמן)
2. חפשו עוד פקטות שיש להם כתובת IP יעד זהה. באיזה פילטר השתמשתם?
3. במהלך ההסנפה בוצעה גלישה לאתר כלשהו. באיזה פילטר תשמשו כדי למצוא את הפקטות הללו?
4. מיצאו לאיזה אתר בוצעה הגלישה. התעלמו מפקטות שמספרן הסידורי קטן מ-400.
5. מהי כתובת ה-IP של האתר אליו בוצעה הגלישה?
6. עשו ping אל כתובת האתר. מהו ה-IP שקיבלתם?
7. מהו הפורט אליו בוצעה הגלישה?
8. מה הפורט של הלקוח?
9. מיצאו פקטת http ששדה ה-content length שלה שווה בדיוק ל-14251 בתים. מה מספר הפקטה?
10. כמה זמן נמשכה הגלישה לאתר? טיפ: בצעו על הפקטה שמצאתם follow TCP stream. מיצאו את שדה ה-date בהודעה הראשונה והאחרונה שהשרת ששלח.