<u>תרגילים</u>

1. ניתוח קובץ
   א. פתח את הקובץ **CaptureFile.cap**.
   ב. כמה חבילות הן בפרוטוקול **HTTP**?
   ג. מתוכן, כמה חבילות ניגשות ל-**host** בשם **www.ynet.co.il**?
   ד. מאיזו כתובת **IP** מגיעות חבילות אלו?
   ה. שמור את החבילות המסוננות בלבד לקובץ בשם **FilteredCapture.cap**.

2. סטטיסטיקות
   א. מה כתובת ה-**MAC** של המחשב ממנו התבצעה ההסנפה?
   ב. כמה כתובות **IP** מופיעות בקובץ?
   ג. איזה אחוז מהחבילות הן בתקן **IPv6**?

3. עבודה עם פילטרים שונים של **Wireshark**
   א. הפעל את **Wireshark**. פתח הסנפה חדשה.
   ב. השתמש במסנן הסנפה (**Capture Filter**) שיסנן אך ורק פניות מהמחשב שלך בפורט 80 של **TCP**. בצע מספר גלישות לאינטרנט. האם המסנן הצליח? רשום את המסנן שבו השתמשת.
   ג. השתמש במסנן הסנפה (**Capture Filter**) כך שיעביר לתוכנה כל חבילה שאינה חבלת **IP**. רשום את המסנן שבו השתמשת.
   ד. השתמש במסנן הסנפה (**Display Filter**) שיסנן רק חבילות מסוג **HTTP POST**. רשום את המסנן שבו השתמשת.
   ה. השתמש במסנן הסנפה (**Display Filter**) שיסנן רק חבילות מסוג **IP** שגודלן עולה על 60 בתים.

4. מחקר בסיסי באמצעות **Wireshark**.
   א. כעת עליך להשתמש במסננים לפי ראות עיניך.
   ב. גלוש אל **YNET**.
   ג. מה כתובת ה-**IP** של האתר?
   ד. כמה בקשות המחשב שלח ל**YNET**?
   ה. כמה תשובות חזרו?
   ו. כמה פקטות נשלחו עם המחרוזת **YNET** שאינן **http**?
   ז. איזה שרת **ynet.co.il** מריץ (האם **apache**? **Microsoft IIS**? **IBM Websphere**?)? באיזו גירסא?

5. מחקר **ping** באמצעות **Wireshark**.
   א. בצע **ping** אל **YNET** על ידי הרצת הפקודה הבאה משורת הפקודה: **ping www.ynet.co.il**
   ב. הבט בחבילות שנשלחו בעקבות הקשת הפקודה וענה על השאלות הבאות (רמז: **ping** משתמש בפרוטוקול **ICMP**):
   ג. מהי כתובת ה-**IP** של **www.ynet.co.il**?
   ד. כמה חבילות בקשה שלחת?
   ה. כמה חבילות תשובה קיבלת?
   ו. מה היה ה-**data** בכל חבילה ששלחת?
   ז. מה היה ה-**data** בכל תשובה שקיבלת?
   ח. איזה שדות ב-**Header** של **ICMP** *זהים* בין שאלה לתשובה?

בהצלחה!