תרגיל: מעקב אחר הודעות שנשלחות ומתקבלות בעת גלישה באינטרנט בעזרת WireShark

יש להדפיס ולמלא בכתב יד את התשובות או לכתוב את התשובות בדף נפרד, לסרוק ולהגיש.
הגשה בכתב היד שלכם בלבד, ובניסוח שלכם. אפשר לחשוב ביחד ולהתייעץ, אבל כל אחד מבין וכותב ומנסח לגמרי לבד.

שם הסטודנט: **תז:**

עכשיו נשתמש בתוכנת WireShark על מנת לעקוב אחר ההודעות שנשלחות ומתקבלות בעת גלישה באתר אינטרנט. כדי לעשות זאת עקוב אחר ההוראות בסעיפים הבאים. (יש למלות בכתב יד)

1. ראשית פתח דפדפן.

2. אם אתה מריץ ממחשב בביתך או ממחשב נייד במכללה התחל להקליט את התקשורת בעזרת WireShark. במידה ואתה מריץ ממחשב של חוות המחשבים במכללה או אם אינך יכול להקליט את התקשורת, פתח בעזרת WireShark קובץ שהוקלט כבר, ומצורף לתרגיל.

3. עבור לכתובת הבאה בדפדפן:
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
הדף שיוצג הוא שורה אחת של מלל.

4. אחרי שהדפדפן הציג את דף האינטרנט שביקשנו (שורה אחת). עצור את ההקלטה ב-WireShark.

5. עכשיו חלון החבילות שנלכדו מכיל פריימים רבים שנשלחו והגיעו למחשבך, ביניהן פריימים של HTTP. כדי להציג דף זה הדפדפן יצר קשר עם שרת ה-HTTP בכתובת gaia.cs.umass.edu, והחליף איתו חבילות תקשורת http.

6. הצג רק את הפריימים של HTTP בעזרת מנגנון ה-display filter:
הקלד http בחלונית התנאי של display filter, בחלק העליון של חלון ה-WireShark, והקש apply.

7. פרוטוקול ה-HTTP עובד כך שדפדן כדי להציג דף אינטרנט, פונה לשרת האינטרנט של אותו האתר, ומבקש שדף האינטרנט של האתר ישלח אליו, ואז מציגו. הבקשה לקבל דף אינטרנט נקראת: HTTP GET.
מצא את חבילת ה-HTTP GET שנשלחה ממחשבך לשרת ה-HTTP gaia.cs.umass.edu. אתה יכול לראות את תפקיד החבילה בשדה ה-info בטבלת החבילות, שם יהיה כתוב:
"GET /wireshark-labs/INTRO-wireshark-files.html HTTP/1.1".
בחר בחבילה וצפה בפירוט של החבילה בחלק האמצעי של חלון WireShark (מתחת לרשימת

החבילות שנלכדו).

8. צפה בפירוט הפריים.
צפה בפירוט השכבות בעזרת לחיצה על ה-'+', וסגור את הפירוט ע"י לחיצה על ה-'-'.
מה הוא הפרוטוקל של שכבת הלינק של פריים זה? Ethernet II
מה הוא הפרוטוקל של שכבת האינטרנט של פריים זה? IPV4
מה הוא הפרוטוקל של שכבת הטרנספורט של פריים זה? TCP
מה הוא הפרוטוקל של שכבת האפליקציה של פריים זה? HTTP
בדוק בשכבת האפליקציה, איזה קובץ ביקש הדפדפן מהשרת בבקשת ה-HTTP GET?
הקובץ INTRO-wireshark-file1.html שהתבקש wireshark-labs

9. כתובת ה-ip היא הכתובת של מחשב ברחבי האינטרנט, ולכן היא הכתובת שמשמשת את שכבת האינטרנט, פרוטוקול ה-IP.
מה כתובת ה-IP של gaia.cs.umass.edu? 128.119.245.12
מה כתובת ה-IP של המחשב שלך? 192.168.10.10

10. מצא את התשובה לבקשת ה-HTTP GET. חבילת התשובה תופיע כמובן אחרי חבילת ה- HTTP GET, אך לא בהכרח בשורה שאחרי. זהה את חבילת התשובה בעזרת בדיקה של כתובת המקור והיעד של החבילה.
יתכנו כמה אפשרויות לתשובה:
במידה שהדף כבר נמצא ב-cahce של מחשבך, תתקבל התשובה not modified, שמשמעותה שהדף שנמצא בזיכרון מחשבך מעודכן, ולכן הדף לא נשלח שנית.
חבילה כזו תסומן בשדה ה-info כך: "HTTP /1.1 304 Not modified"
אם אין דף מעודכן ב-cache של מחשבך, ולא היתה בעיה בבקשת ה-HTTP GET, תתקבל תשובה HTTP OK עם תוכן דף האינטרנט הדרוש.
חבילה כזו תסומן בשדה ה-info כך: "HTTP /1.1 200 ok"
הקף איזו תשובה התקבלה מהשרת? Not modified / HTTP OK
אם התקבל HTTP OK, מצא את התוכן של דף האינטרנט בפירוט שכבת פרוטוקול ה-HTTP.

11. כמה זמן עבר בין שליחת הודעת ה-HTTP GET ועד לקבלת התשובה? (ברירת המחדל של עמודת הזמן ברשימת החבילות ב-WireShark הוא הזמן בשניות שעבר מאז שהתחילה הלכידה)
3.205532 - 3.042194 = 0.163338