מעבדה 1: HTTP & DNS

רקע

"אני שומע - ושוכח. אני רואה – וזוכר. אני עושה – ומבין" (מיוחס לקונפוציוס).
מטרת המעבדות בקורס היא "לראות בעיניים" דוגמאות של החומר הנלמד בקורס. Wireshark הוא כלי חינמי ופשוט, שמאפשר לנטר את כל החבילות שהמחשב שולח ומקבל.
כהיכרות עם Wireshark, יש להיעזר בקובץ העזר "מבוא ל-Wireshark" שבאתר. **אין צורך להגיש את המטלות המתוארות שם.**

הערות:

- מאחר שכאמור, Wireshark מנטר את **כל** החבילות, כדאי למעט בחבילות שיוצרות "רעש" ואינן רלבנטיות לתרגיל – ולפיכך מומלץ להשאיר רק דפדפן אחד פתוח עם לשונית אחת בעת ביצוע התרגיל. בפועל – גם כך סביר שינוטרו חבילות שלא קשורות לתרגיל בשל תהליכי רקע שונים שרצים במחשב, ושולחים ומקבלים חבילות (עדכוני תוכנה, סנכרון קבצים של Google Drive / Dropbox וכיו"ב).
- התרגיל הוא מעבדה שאין לה "פתרון בית ספר" נכון יחיד. לסטודנטים שונים יכולות, ואף צריכות, להתקבל תוצאות שונות.
- כדי להעתיק ולהדביק נתונים מתוך החבילות ב-Wireshark יש ללחוץ בלחיץ ימין של העכבר על השדה שרוצים להעתיק, ואז לבחור Copy → Values.
- בגלל השימוש בזכרונות מטמון יתכנו הבדלים בין הגישה הראשונה ל-URL מסוים, לבין הגישות הבאות לאותו URL. לפיכך, עליך לשמור את הנתונים שניטר Wireshark באמצעות File → Save, כדי שתוכל/י לגשת אליהם שוב בהמשך.
- יש לצרף צילום מסך מ-Wireshark לכל אחת מהשאלות 1,2,3. מספיק צילום יחיד לכל השאלה (אין צורך בצילום לכל סעיף בנפרד) – אך במידת האפשר יש למזער את השדות שאינם רלבנטיים, לגלול ולסדר את המידע כך שמירב הנתונים הרלבנטיים יופיעו בצילום.
- **אני מקווה שיהיה לכם מעניין לפתור את המעבדה, כפי שהיה לי מעניין להכין אותה בעצמי ולכתוב את השאלות ☺.**

במעבדה זו נבחן חלק מהחבילות הנשלחות כאשר אנו מנסים לגשת לאתרים שונים. כדי למעט בחבילות "רעש" שאינן רלבנטיות לתרגיל, מומלץ בכ"א מהשאלות סדר הפעולות הבא:

1. לפתוח את Wireshark ודפדפן אינטרנט (אם הם לא היו פתוחים קודם), ובו לשונית אחת ריקה (ללא דף מסוים). אם יש לשוניות פתוחות שמציגות אתרים מסוימים, כגון דף הבית, ניתן לפתוח לשונית נוספת ריקה, ואז לסגור את כל הלשוניות האחרות.
2. להקליד בדפדפן את הכתובת המתוארת בשאלה, **בלי להוסיף www. לפניה, ומבלי ללחוץ ENTER** (כדי לא לטעון אותה, אלא רק להיות מוכנים לעשות זאת במהירות בהמשך).
3. ללחוץ Start ב-Wireshark כדי להתחיל ליירט חבילות.
4. ללחוץ ENTER בדפדפן, כדי לטעון את הדף.
5. להמתין עד שיעלה הדף המתאים - או הודעת שגיאה, כגון "הדף לא נמצא". יש להמתין לעלייה **הסופית** של הדף, לאחר הודעות כגון "מפנה מחדש" (Redirecting).
6. ללחוץ Stop ב-Wireshark.

שאלות

1. יש להקליד בשורת הכתובת את שתי הספרות האחרונות בתעודת הזהות שלך (אם מגישים את התרגיל בזוג, ניתן לבחור מספר ת.ז. של אחד הסטודנטים), ואז com.
לדוגמא, אם תעודת הזהות שלך מסתיימת ב-"12", יש להקליד 12.com.
א. מהי כתובת ה-IP של המחשב שלך?
ב. מהי כתובת ה-IP של שרת ה-DNS המקומי של המחשב שלך?
ג. האם הכתובת שהקלדת מציינת כתובת URL קיימת? אם כן, מהי כתובת ה-IP של השרת שמאחסן אותה?

ד. צייני שם וכתובת IP של שרת מורשה (authoritative nameserver) של ה-URL שהקלדת.
ה. על גבי איזה פרוטוקול של שכבת התעבורה (transport) שלח המחשב שלך את בקשת ה-DNS?

2. יש להקליד בשורת הכתובת: www.opnet.com
א. מהי כתובת ה-IP של השרת שאליו הצביעה התשובה הראשונה שקיבלת משרת ה-DNS המקומי?
ב. מהי כתובת ה-IP של השרת שעליו מאוחסן דף האינטרנט בפועל?
ג. מהו ה-URL הקנוני של האתר המשויך לURL-www.opnet.com?
ד. כמה זמן חלף מרגע שהמחשב שלך שלח את בקשת ה-DNS **הראשונה** עבור הכתובת הנ"ל ועד שהתקבלה תשובת ה-DNS שמכילה את הכתובת שבה מאוחסן הדף בפועל?
ה. כמה זמן חלף מרגע שהמחשב שלך שלח את בקשת ה-HTTP הראשונה עבור הדף, עד שהתקבלה התשובה הראשונה מהשרת שמאחסן את הדף בפועל?
ו. פתח לשונית חדשה, הקלד בה שוב 123.com (מבלי ללחוץ ENTER), וסגור את הלשונית הקודמת. הפעל שוב את Wireshark כפי שתואר במבוא לתרגיל, כדי ליירט את החבילות הנשלחות עבור בקשה החדשה.
ז. כמה זמן חלף הפעם מרגע שהמחשב שלך שלח בקשת DNS או HTTP עבור הבקשה, ועד שהתקבלה תשובת ה-HTTP מהשרת שמאחסן את הדף בפועל?
ח. נסי להעריך באיזה מהשיטות שנלמדו בהרצאה נעשה שימוש כדי לייעל את הגישה החוזרת לאתר מוכר. הסבירי בקצרה.

3. יש להקליד בשורת הכתובת
https://www.youtube.com/watch?v=loncOoEbLQY
מומלץ גם (אבל לא חובה...) לצפות בסרטון ☺.
א. האם היישום משתמש בחבילות TCP או ב-UDP?
ב. מהם היתרונות בשימוש ב-UDP לצורך יישומי זמן אמת ו-streaming?
ג. ציינו חיסרון אחד, שמקשה על השימוש ב-UDP.

4. קרא על צינור (pipelining) של בקשות ב-HTTP/1.1 ב-RFC 7230, פרק 6.3.2 – למשל, בכתובת:
http://tools.ietf.org/html/rfc7230#section-6.3.2
א. איזה פעולות מוגדרות כ "בטוחות" (safe methods)?
ב. מדוע אסור לשרת לבצע במקביל מספר גישות שאינן בטוחות שמבקש לקוח מסוים? תן דוגמא לנזק שעלול להיגרם אם השרת יבצע פעולות במקביל פעולות שאינן בטוחות.
ג. איזה חלק מהטיפול בבקשת הלקוח מותר לשרת לבצע באופן מקבילי, כאשר מדובר בפעולות בטוחות? מדוע?
ד. איזה חלק מהטיפול חייב להתבצע באופן טורי בכל מקרה, גם כאשר מדובר בפעולות בטוחות?