שיעור 4 – מודל השכבות והיכרות עם Wireshark

תרגיל: כלי מזג-אוויר

בתרגיל זה נשתמש בתוכנה מוכנה אשר משתמשת באינטרנט. כדי להבין את פעולת התוכנה נצטרך ללכת אל מאחורי הקלעים – בעזרת תוכנת Wireshark – כדי לגלות מה באמת שולחת ומקבלת התוכנה מהאינטרנט. לאחר מכן נשתמש בטלנט כדי לדבר בעצמנו את הפרוטוקול מול השרת.

1. הורדת תוכנה

הורידו את הקובץ של תוכנת מזג האוויר (WeatherClient.rar) מתיקיית תכני השיעור. פתחו (Extract) את קובץ ה-Rar לתוך תיקיה והיכנסו לתוך התיקיה.

**שימו לב, לא מפעילים תוכנות מתוך ה-RAR עצמו!**

**עזרה:** כדי לפתוח קבצי rar מומלץ להשתמש בתוכנת Winrar. נסו ללחוץ כפתור ימני על קובץ ה-rar, ואז לבחור ב-**"Extract to “WeatherClient\.** כעת תיפתח תיקייה חדשה בשם WeatherClient שהקבצים נמצאים בתוכה. היכנסו אליה.

2. בדיקת ה**-IP** שלנו

1. בעזרת פקודת ipconfig, בדקו מהו ה-IP של המחשב שלכם ורשמו אותו:

|  |
| --- |
| 192.168.1.102 |
| *תשובה* |



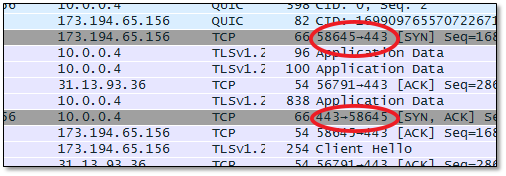
3. הרצה ראשונה של התוכנה

1. לחצו פעמיים על הקובץ WeatherClient.   
   **(לא להריץ את התוכנה מתוך** Winrar**!)**  
     
   אתם אמורים לראות את התוכנה נפתחת במסך הבא:
2. כעת ננסה להבין מדוע התוכנה לא פועלת. סגרו את תוכנת מזג האוויר, ופתחו את Wireshark.
3. כדי שנוכל לראות את תעבורת התוכנה ולהתעמק בה, עלינו למצוא את הפילטר הנכון שיבודד רק את התעבורה הזאת. כדי לעשות זאת, נסו לוודא שכמה שפחות תוכנות משתמשות באינטרנט במחשב. התחילו בהסנפה ומיד לאחר מכן הפעילו את תוכנת מזג האוויר. הפסיקו את ההסנפה **מיד לאחר** שהתוכנה נפתחת – כמה שיותר מהר!
4. נסו לגלות מהו ה-IP איתו מתקשרת התוכנה שלנו. זהו IP שחוזר מספר פעמים והוא לא ה-IP שלנו. בעזרת מדריך הפילטרים הנפוצים ל-Wireshark, כתבו סינון אשר מציג רק את החבילות **היוצאות והנכנסות** ל-IP הזה. אם כתבתם פילטר נכון, אתם אמורים לראות כעת רק את התעבורה של תוכנת מזג האוויר. כתבו את הסינון אשר כתבתם:

|  |
| --- |
| ip.addr == 34.218.16.79 |
| *תשובה* |

**\* טיפ:** כדי לוודא שהפילטר שלכם באמת "תפס" את התוכנה, המשיכו להסניף בזמן שהפילטר קיים. שימו לב שבכל הרצה מחודשת של התוכנה מתווספות חבילות נוספות לתצוגה.

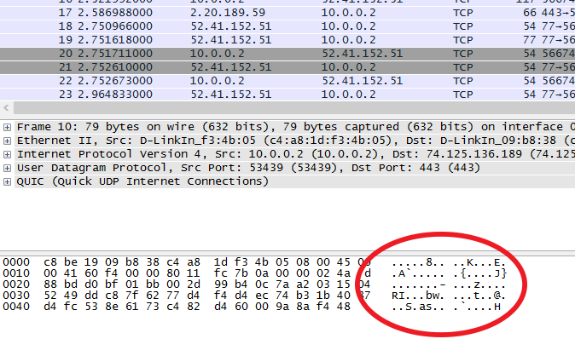
1. לאחר שמצאתם את ה-IP, חפשו מהו הפורט הפתוח אצל השרת איתו אנו מדברים? מהו הפורט שפתחנו אצלנו (לקוח)? זכרו, הפורטים מופיעים כך (שימו לב שהכיוון של החץ קשור לחבילה שבחרתם – אם היא יוצאת מהמחשב או נכנסת מהמחשב):



|  |
| --- |
| הפורט של השרת :77  הפורט שלי(לקוח) 10439 |
| *תשובה* |

1. צרו סינון נוסף אשר מבודד את התעבורה של תוכנת מזג האוויר בלבד, הפעם על בסיס הפורט. כלומר, פילטר נוסף אשר יציג את אותן תוצאות כמו הפילטר מסעיף ד'. כתבו את הסינון אשר כתבתם:

|  |
| --- |
| tcp.port == 77 |
| *תשובה* |

1. כעת אמורות להיות מוצגות כ-20 חבילות לכל היותר על המסך. נסו לעבור בין החבילות עם החצים למעלה ולמטה במקלדת, בעוד אתם מסתכלים על החלונית התחתונה ביותר של Wireshark המציגה את תוכן החבילה. חפשו חבילה הכוללת תוכן טקסטואלי.  
   
2. נסו לחפש את השגיאה אשר חזרה מהשרת וכתבו אותה כאן:

|  |
| --- |
| 500:ERROR:date illegal: date is in the past or format is invalid |
| *תשובה* |

1. עדיין ב-Wireshark, נסו לחפש את החבילה הכוללת את המידע אשר נשלח מהמחשב שלנו וגרם לשרת לשלוח את השגיאה. כתבו את המידע ונסו להסביר מדוע לדעתכם התקבלה שגיאה?

|  |
| --- |
| 100:REQUEST:city=Eilat&date=11/09/2018&checksum=47.22  ככול הנראה בגלל שהתאריך בעבר |
| *תשובה* |

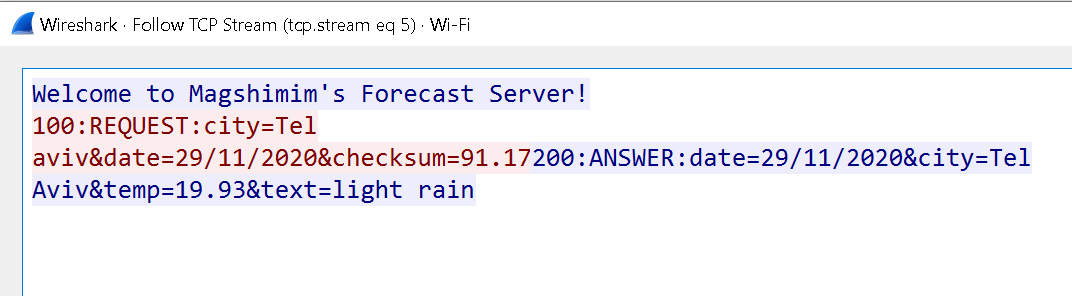
1. חזרו לתיקיית התוכנה. נסו לחפש מאיפה מגיע המידע אשר גורם לשגיאה. נסו לשנות אותו ולגרום לתוכנה לעבוד ולהחזיר תחזית מזג אוויר אמיתית. צרפו כאן צילום מסך של התוכנה כאשר היא פועלת כהלכה (ב-Word ניתן לצלם את המסך בעזרת תפריט הוספה->צילום מסך).



1. התחילו הסנפה חדשה. נסו לשנות את העיר לעיר אחרת לבחירתכם (מישראל או מהעולם) וצרפו צילום מסך.   
   



1. פתחו את חלון Follow TCP Stream אשר מציג את השיחה עם השרת. צרפו צילום מסך.



שימו לב, שלמרות שבחלון ה-Follow TCP Stream מוצגות רק 3 הודעות שעברו בין הצדדים, יש יותר חבילות בפועל שעברו בין שני הצדדים. נלמד מדוע זה קורה בהמשך הקורס.

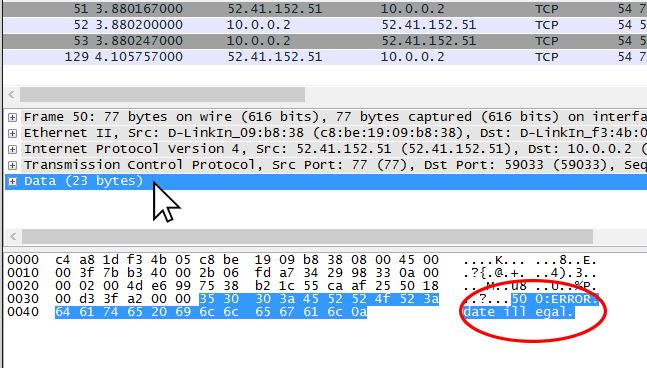
1. נסו להבין מהו טווח הימים שניתן להכניס בשדה התאריך, וכתבו כאן הסבר למה קיים טווח שכזה לדעתכם:

|  |
| --- |
| 5 ימים כי התוכנה לא יכולה לחזות ליותר מזה |
| *תשובה* |

4. אבחון הפרוטוקול

כפי שלמדנו בשיעור הראשון, פרוטוקול הוא למעשה שפה הכוללת סט מוגדר של חוקים לשיחה ברשת. כעת ננסה ללמוד את הפרוטוקול בו משתמשת תוכנת מזג האוויר.

**עזרה**: לשם כך נמשיך להתמקד בחלק התחתון ביותר של Wireshark המציג את תוכן החבילה. כדי לפשט את העבודה, נוכל להגיד ל-Wireshark לסמן לנו את החלק הרלוונטי בכחול. כדי לעשות זאת, בכל חבילה שנבחר, נעבור למסך האמצעי (מסך השכבות) ונלחץ על השורה התחתונה ביותר בו, Data. כעת נוכל לראות שהחלק המעניין מסומן למטה מצד ימין בכחול.

.

כתבו הסבר על ההודעות של הפרוטוקול בעזרת הטבלה הבאה.

בסעיף **"מבנה הודעה"** יש לכתוב איך כתובה ההודעה. אם זיהיתם חלק בהודעה שמשתנה ואינו קבוע, תוכלו לצין אותו בעזרת <>, באופן דומה למה שעשינו בתרגיל "המבורגר בענן". למשל: GETWEATHER:<CITY>:<DATE>

בסעיף **"הסבר"** יש להסביר את מטרת ההודעה לדעתכם, ולהסביר את כל השדות ששמתם ב-<>.

|  |  |
| --- | --- |
| **הודעת פתיחה (שרת -> לקוח)** | |
| מבנה הודעה | Welcome to Magshimim's Forecast Server! |
| הסבר | השרת אומר שלום |
| **בקשה (לקוח -> שרת)** | |
| מבנה הודעה | 100:REQUEST:<city>&<date>&<checksum> |
| הסבר | <city> העיר שרוצים <date> התאריך שרוצים לקבל את התחזית עליו  <checksum> בדיקה שהנתונים תיקניים |
| **תשובה (שרת -> לקוח)** | |
| מבנה הודעה | 200:ANSWER:<date>&<city>&<temp>&<text> |
| הסבר | <date> זה התאריך שביקשנו בבקשה <city>זה העיר שביקשנו בבקשה  <temp> זה הטמפרטורה שהשרת החזיר <text> תיאור של מזג האוויר במילים |
| **הודעת שגיאה (שרת->לקוח)** | |
| מבנה הודעה | 500:ERROR:<תיאור של השגיאה> |
| הסבר | זה אומר מה הבעיה |

5. פענוח שדה ה-**Checksum**

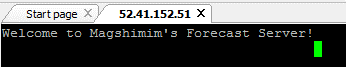
1. שדה ה-checksum הוא שדה אשר מהווה בדיקה שכל המידע בבקשה עבר כהלכה. כדי לעשות זאת הוא מבצע פעולה מתמטית על המידע של הבקשה ושולח את התוצאה הזאת יחד עם המידע. במקרה שלנו ה-checksum מורכב משני חלקים – החלק הראשון מבצע פעולה מתמטית על שדה העיר, והחלק השני מבצע פעולה מתמטית על התאריך.
2. כעת ננסה יחד לפענח את החלק השני, הקשור לתאריך. כדי לעשות זאת, נשלח בעזרת התוכנה מספר 3 בקשות שונות, שבכל אחת יש הבדל קטן בתאריך. כתבו את התאריך ואת הצ'קסאם שהוא יצר:

|  |
| --- |
| תאריך: 3/12/2020  Checksum: 10  תאריך: 2/12/2020  Checksum: 9  תאריך:1/12/2020  Checksum:8 |
| *תשובה* |

1. נסו לבחון את ההבדלים בין ה-Checksums וכיצד הם קשורים לתאריכים השונים. לאחר שהבנתם כיצד מחושב החלק השני של ה-checksum, הסבירו זאת:

|  |
| --- |
| החלק השני זה סכום המספרים בתאריך |
| *תשובה* |

6. התחברות לשרת ב-**Telnet**

1. כעת נרצה אנחנו להחליף את תפקיד התוכנה ולדבר בעצמנו עם שרת מזג האוויר. לשם כך אנו זקוקים ל-IP ולפורט בו התוכנה פונה אל השרת (הפורט שמעניין אותנו הוא הפורט בצד השרת אשר נשאר תמיד קבוע ולא הפורט שנפתח אצלנו שהוא אקראי).
2. בעזרת תוכנת PuttyTM, ניצור חיבור חדש עם הפרטים של שרת מזג האוויר. אם שכחתם איך עושים זאת, פתחו שוב את תרגיל הכיתה של שיעור 2.
3. אם התחברתם בהצלחה, תראו את ההודעה הבאה:
4. אם לא הצלחתם להתחבר בדקו שבחרתם את ה-IP והפורט הנכונים שוב.
5. שלחו לשרת את ההודעה "Hello" וכתבו מה התשובה שהוא שלח:

|  |
| --- |
| 500:ERROR:arguments invalid |
| *תשובה* |

🞺 **טיפ:** כדי להעתיק טקסט ב-Putty יש לסמן את הטקסט וללחוץ על כפתור ימני בעכבר.  
כדי להדביק נלחץ על כפתור ימני בעכבר.

🞺 **טיפ2:** כדאי להיעזר בתוכנת עריכת טקסט לעריכת ההודעות כדי לא לכתוב אותן מחדש בכל פעם.

1. התחברו שוב והפעם כתבו לשרת הודעה חוקית (הודעה זהה לחלוטין לאחת שהסנפתם מהפעולה של התוכנה). אם לא קיבלתם תשובה נסו מספר פעמים נוספות. אם הצלחתם לקבל תשובה, כתבו את ההודעה ששלחתם וצרפו צילום מסך של התשובה של השרת.

|  |
| --- |
| 100:REQUEST:city=Tel aviv&date=1/12/2020&checksum=91.8 |
| *תשובה* |

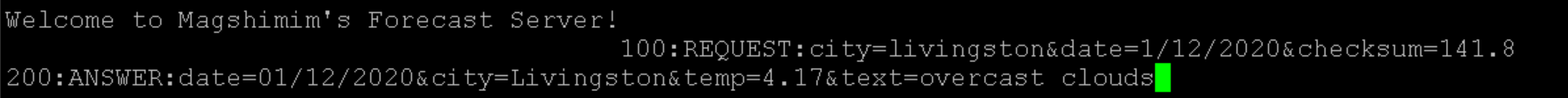


1. כתבו הודעה זהה מלבד שדה אחד: בקשו את התאריך של אתמול. זכרו, כעת גם ה-Checksum צריך להתעדכן. כתבו מה ההודעה שהשרת החזיר:

|  |
| --- |
| 500:ERROR:date illegal: date is in the past or format is invalid |
| *תשובה* |

1. בונוס**:** בחרו עיר בעולם הקרובה לליבכם, ובקשו את התחזית שלה ב-telnet. לא חובה לכתוב את שם המדינה, ניתן לכתוב רק שם של עיר. שימו לב, כדי לעשות זאת תצטרכו לפענח את החלק הראשון של ה-Checksum בעצמכם, ללא עזרת התוכנה! אם הצלחתם, צרפו צילום מסך והסבירו כיצד מחושב החלק הראשון של ה-Checksum.





|  |
| --- |
| Checksum זה הסכום של הגימטריה כש A=1 B=2...Z=26ד |
| *תשובה* |