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:

| 192.168.56.1 |
| --- |
| *תשובה* |



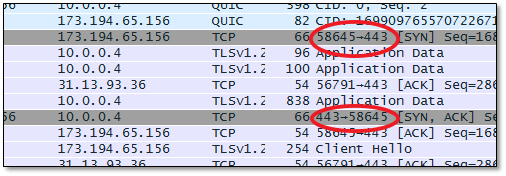
3. הרצה ראשונה של התוכנה

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.

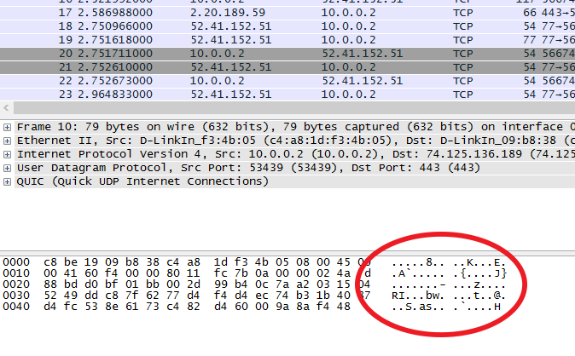
1. לאחר שמצאתם את ה-IP, חפשו מהו הפורט הפתוח אצל השרת איתו אנו מדברים? מהו הפורט שפתחנו אצלנו (לקוח)? זכרו, הפורטים מופיעים כך (שימו לב שהכיוון של החץ קשור לחבילה שבחרתם – אם היא יוצאת מהמחשב או נכנסת מהמחשב):



| פתוח שלי: 60605, פתוח שלו:77 |
| --- |
| *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.srcport == 77 or tcp.srcport == 60605 |
| --- |
| *תשובה* |

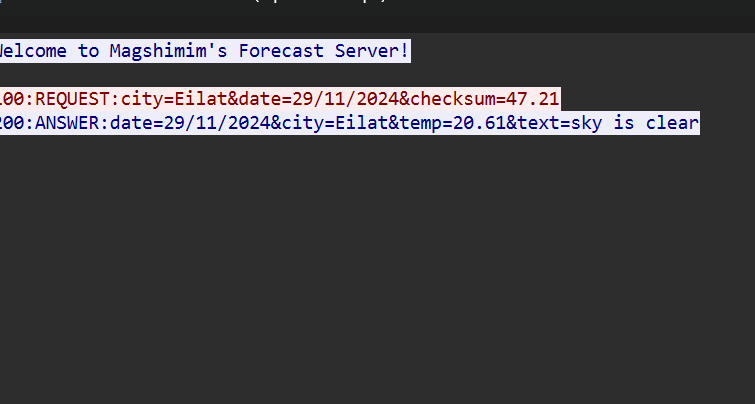
1. כעת אמורות להיות מוצגות כ-20 חבילות לכל היותר על המסך. נסו לעבור בין החבילות עם החצים למעלה ולמטה במקלדת, בעוד אתם מסתכלים על החלונית התחתונה ביותר של Wireshark המציגה את תוכן החבילה. חפשו חבילה הכוללת תוכן טקסטואלי.  
   
2. נסו לחפש את השגיאה אשר חזרה מהשרת וכתבו את ההודעה כאן (שימו-לב: המספר בתחילת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

| 0000 20 0b 74 26 7c fc 28 d1 27 4d 25 1f 08 00 45 00 .t&|.(.'M%...E.  0010 00 69 85 26 40 00 65 06 7c e1 22 da 10 4f c0 a8 .i.&@.e.|."..O..  0020 1f b6 00 4d ec bd e7 3a 63 27 cf 3e 59 a7 50 18 ...M...:c'.>Y.P.  0030 01 f6 81 57 00 00 35 30 30 3a 45 52 52 4f 52 3a ...W..500:ERROR:  0040 64 61 74 65 20 69 6c 6c 65 67 61 6c 3a 20 64 61 date illegal: da  0050 74 65 20 69 73 20 69 6e 20 74 68 65 20 70 61 73 te is in the pas  0060 74 20 6f 72 20 66 6f 72 6d 61 74 20 69 73 20 69 t or format is i  0070 6e 76 61 6c 69 64 0a nvalid. |
| --- |
| *תשובה* |

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

| 500:ERROR:date illegal: date is in the past or format is invalid.  הבעיה שכתוב תאריך לא נכון בקוד של הכלי המזג האוויר. |
| --- |
| *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).  
    
2. התחילו הסנפה חדשה. נסו לשנות את העיר לעיר אחרת לבחירתכם (מישראל או מהעולם) וצרפו צילום מסך (צילום מסך של האפליקציה, כמו בסעיף הקודם).   
   
3. 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.

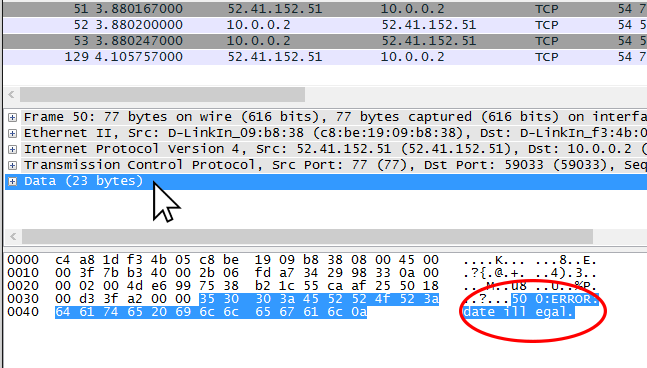
1. נסו להבין מהו טווח הימים שניתן להכניס בשדה התאריך, כתבו מהו הטווח והסבירו למה קיים טווח שכזה לדעתכם:

| הטווח הוא שלושה ימים קדימה והיום, הטווח הוא כזה כדי שעם יהיה טווח ארוך יותר לשרת יהיה עומס הרבה יותר גדול והוא יכול לקרוס, ובנוסף יהיה קשה מאוד לדעת את המזג האוויר לתאריך ארוך יותר. |
| --- |
| *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 | פשוט המשפט פתיחה של שרת |
| **בקשה (לקוח -> שרת)** | |
| מבנה הודעה | 100:REQUEST:<city=Eilat>&<date=29/11/2024>&<checksum=47.21> |
| הסבר | בקשה של המזג האוויר שבאילת בתאריך 29/11/2024 |
| **תשובה (שרת -> לקוח)** | |
| מבנה הודעה | 200:ANSWER:<date=29/11/2024>&<city=Eilat>&<temp=20.61>&<text=sky is clear> |
| הסבר | תשובה שמראת שבאילת ב29/11/2024 הטמפ היא 20.61 מאלות ושהשמיים נקיים |
| **הודעת שגיאה (שרת->לקוח)** | |
| מבנה הודעה | 500:ERROR:<date illegal: date is in the past or format is invalid.> |
| הסבר | הודעה אומרת שהזמן שנותן הוא זמן בעבר או שסוגו לא נכון. |

5. פענוח שדה ה-**Checksum**

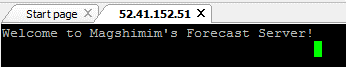
1. שדה ה-checksum הוא שדה אשר מהווה בדיקה שכל המידע בבקשה עבר כהלכה. כדי לעשות זאת הוא מבצע פעולה מתמטית על המידע של הבקשה ושולח את התוצאה הזאת יחד עם המידע. במקרה שלנו ה-checksum מורכב משני חלקים – החלק הראשון מבצע פעולה מתמטית על שדה העיר, והחלק השני מבצע פעולה מתמטית על התאריך.
2. כעת ננסה יחד לפענח 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: 29.11.2024  Checksum:checksum=63.21  תאריך:30.11.2024  Checksum:checksum=63.13  תאריך:01.12.2024  Checksum:checksum=63.12 |
| --- |
| *תשובה* |

1. נסו לבחון את ההבדלים בין ה-Checksums וכיצד הם קשורים לתאריכים השונים. נסו לשלוח הודעות נוספות עם תאריכים שונים, נסו לשנות חלקים שונים של התאריך, כדי להבין את החוקיות. לאחר שהבנתם כיצד מחושב החלק השני של ה-checksum, הסבירו זאת:

| המספר שאחרי הנקודה זה הסכום של כול 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:

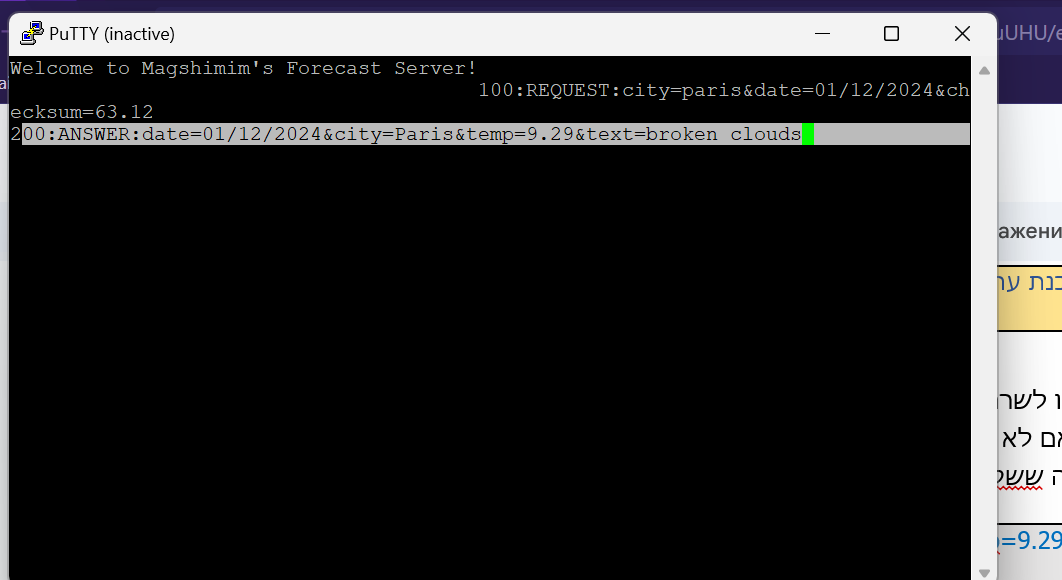
| השרת פשוט סגר את החיבור. |
| --- |
| *תשובה* |

🞺 **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**.

| 00:ANSWER:date=01/12/2024&city=Paris&temp=9.29&text=broken clouds |
| --- |
| *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.



|  |
| --- |
| *תשובה* |

