שיעור 3 – 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)) מהקישור ב-Edu. פתחו את קובץ ה-Rar לתוך תיקיה והיכנסו לתוך התיקיה.

**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:

|  |
| --- |
| 10.7.8.196 |
| תשובה |



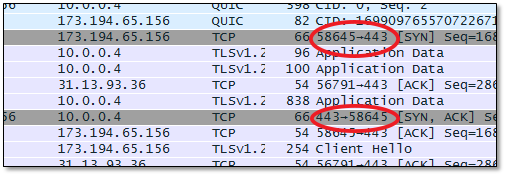
**3. הרצה ראשונה של התוכנה**

1. לחצו פעמיים על הקובץ WeatherClient. אתם אמורים לראות את התוכנה נפתחת במסך הבא:
2. כעת ננסה להבין מדוע התוכנה לא פועלת. סגרו את תוכנת מזג האוויר, ופתחו את Wireshark. כדי לבודד את התעבורה שמעניינת אותנו, 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!
3. 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  ip.dst == 34.218.16.79 or ip.src == 34.218.16.79 |
| תשובה |

**\* טיפ:** כדי לוודא שהפילטר שלכם באמת "תפס" את התוכנה, שימו לב שבכל הרצה מחודשת של התוכנה מתווספות חבילות לתצוגה

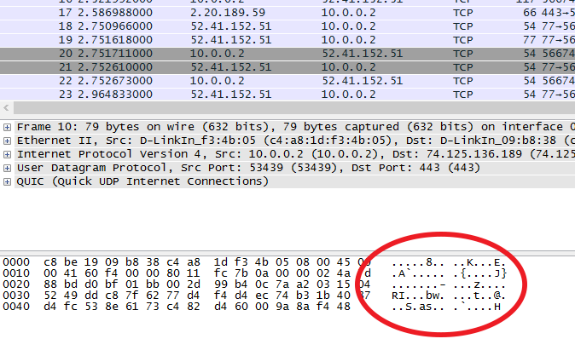
1. לאחר שמצאתם את ה-IP, חפשו מהו הפורט הפתוח אצל השרת איתו אנו מדברים? מהו הפורט שפתחנו אצלנו (לקוח)? זכרו, הפורטים מופיעים כך (שימו לב שהכיוון של החץ קשור לחבילה שבחרתם – אם היא יוצאת מהמחשב או נכנסת מהמחשב):



|  |
| --- |
| 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.dstport==77 or tcp.srcport==77 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:

|  |
| --- |
| הודעת הפתיחה של השרת אלינו היא:  Welcome to Magshimim's Forecast Server!  ואחריה נשלחת הודעה מאיתנו לשרת, ותגובתו היא הודעת השגיאה הבאה:  500:ERROR:date illegal: date is in the past or format is invalid |
| תשובה |

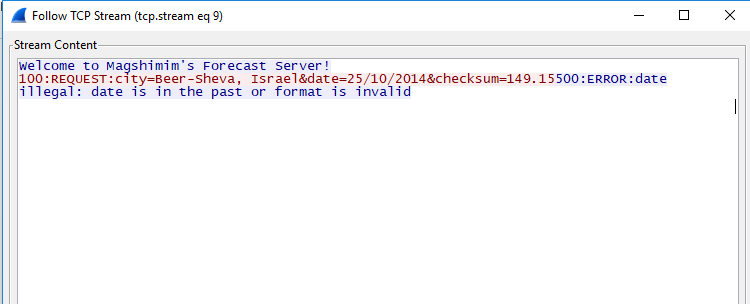
1. עדיין ב-Wireshark, נסו לחפש את החבילה הכוללת את המידע אשר נשלח מהמחשב שלנו וגרם לשרת לשלוח את השגיאה. כתבו את המידע ונסו להסביר מדוע לדעתכם התקבלה שגיאה?

|  |
| --- |
| ההודעה ששלחנו אנחנו לשרת היא:  100:REQUEST:city=Beer-Sheva, Israel&date=25/10/2014&checksum=149.15  הסיבה לקבלת השגיאה היא שהתאריך שהזנו הוא לא חוקי (הוא מהעבר). |
| 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.   
   
2. פתחו את חלון Follow TCP Stream אשר מציג את השיחה עם השרת. צרפו צילום מסך.



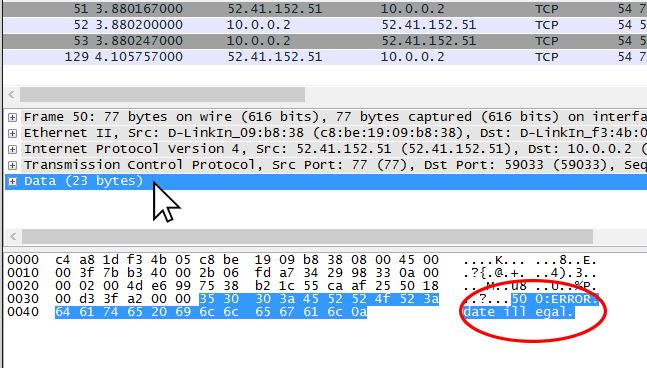
שימו לב, שלמרות שבחלון ה-Follow TCP Stream מוצגות רק 3 הודעות שעברו בין הצדדים, יש יותר חבילות בפועל שעברו בין שני הצדדים. נלמד מדוע זה קורה בהמשך הקורס.

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

|  |
| --- |
| טווח התאריכים הוא מהיום ועד עוד ארבעה ימים, והסיבה היא שלא ניתן לקבל נתונים אמינים על יותר מארבעה ימים קדימה (וחיפוש על ימים מהעבר אינו רלוונטי עבור התוכנה הספציפית הזאת). |
| 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:

בסעיף **"כיצד היא נראית"** יש לכתוב בדיוק את ההודעה כפי שהיא. אם זיהיתם חלק בהודעה שמשתנה ואינו קבוע, תוכלו לצין אותו בעזרת <>. למשל: GETWEATHER:<CITY>:<DATE>

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

|  |  |
| --- | --- |
| **הודעת פתיחה (שרת -> לקוח)** | |
| כיצד היא נראית? | Welcome to Magshimim's Forecast Server! |
| הסבר | הודעת פתיחה מהשרת למשתמש. |
| **בקשה (לקוח -> שרת)** | |
| כיצד היא נראית? | 100:REQUEST:city=<CITY, COUNTRY>&date=<DATE>&checksum=<CHECKSUM> |
| הסבר | החלק הראשון זה מספר המייצג שמדובר בבקשת מידע על מזג אוויר מהשרת. אחריו מגיעים שלושה שדות שהם העיר, התאריך וה-checksum, והשדות הללו מופרדים ב"&". |
| **תשובה (שרת -> לקוח)** | |
| כיצד היא נראית? | 200:ANSWER:date=<DATE>&city=<CITY>&temp=<TEMPERATURE>&text=<TEXT> |
| הסבר | במידה והבקשה מהלקוח תקינה, מוחזרת הודעה עם קוד 200 (קוד תגובה תקינה) ואז ארבעה שדות שהם התאריך, העיר, הטמפרטורה וההודעה שיש להציג למשתמש, מופרדים ע"י "&". |
| **הודעת שגיאה (שרת->לקוח)** | |
| כיצד היא נראית? | 500:ERROR:<ERROR MESSAGE> |
| הסבר | במידה והייתה בעיה בבקשה מהמשתמש, מוחזרת הודעה עם קוד 500 (קוד של שגיאה) ואחריו הודעת השגיאה (במקרה של תאריך שגוי, date illegal). |

**5. פענוח שדה ה-Checksum**

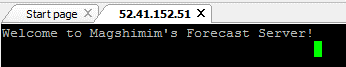
1. שדה ה-checksum הוא שדה אשר מהווה בדיקה שכל המידע בבקשה עבר כהלכה. כדי לעשות זאת הוא מבצע פעולה מתמטית על המידע של הבקשה ושולח את התוצאה הזאת יחד עם המידע. במקרה שלנו ה-checksum מורכב משני חלקים – החלק הראשון מבצע פעולה מתמטית על שדה העיר, והחלק השני מבצע פעולה מתמטית על התאריך.
2. כעת ננסה יחד לפענח 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: 26.10.2017  Checksum: 149.19  תאריך: 27.10.2017  Checksum: 149.20  תאריך: 28.10.2017  Checksum: 149.21 |
| 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:

|  |
| --- |
| שדה checksum הוא שדה מקובל בפרוטוקולי תקשורת ואנו ניתקל בו לא מעט במהלך הקורס. מטרתו היא לאפשר לצד השני לוודא שהמידע שאנחנו שולחים לא השתבש בדרך. לרוב ה-checksum הוא בעצם פעולה מתמטית שמתבצעת על המידע שנשלח, והתוצאה של הפעולה הזו נשלחת יחד עם המידע, ככה שהצד השני יוכל לבצע את אותה הפעולה על המידע ולראות אם התוצאה שלו תואמת את התוצאה שנשלחה אליו. אם התוצאה לא תואמת, הצד המקבל יודע להגיד שהמידע הגיע בצורה משובשת, ולכן עליו להתעלם ממנו או לבקש את המידע מחדש.  במקרה שלנו, ה-checksum מורכב משני מספרים המופרדים בנקודה. החלק השני שמתייחס לתאריך הוא סכום הספרות שנמצאות בתאריך (28.10.2017 זה 21, למשל).  השרת שמקבל את הבקשה שלנו יכול בקלות לסכום את הספרות והאותיות ולוודא שה-checksum שיצא לו זהה ל-checksum שאנחנו שלחנו עם הבקשה. |
| 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. נפתח את תוכנת ה-Telnet שלנו (PuttyTM) ונלחץ על כפתור ההגדרות:
3. ניצור חיבור חדש עם הפרטים של שרת מזג האוויר. אם שכחתם איך עושים זאת, פתחו שוב את תרגיל הכיתה של שיעור 2.
4. נשמור את האתר בעזרת Saved Sessions. נצא ממסך ההגדרות ונחזור לתוכנה PuttyTM.
5. אם שמרנו את האתר כהלכה, הוא יופיע כשנלחץ על הכפתור:
6. נלחץ פעמיים על שם האתר כדי להתחבר אליו.
7. אם התחברתם בהצלחה, תראו את ההודעה הבאה:
8. אם לא הצלחתם להתחבר בדקו שבחרתם את ה-IP והפורט הנכונים שוב.
9. שלחו לשרת את ההודעה "Hello" וכתבו מה התשובה שהוא שלח:

|  |
| --- |
| ההודעה ששלחנו איננה כלולה בפרוטוקול ולכן השרת לא יודע מה לעשות איתה. במצב כזה הוא מתוכנת להחזיר לנו תגובת שגיאה כללית: |
| 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.

|  |
| --- |
| נשלח את הבקשה הבאה:  100:REQUEST:city=Ofaqim, Israel&date=25/10/2016&checksum=125.17  ונקבל את התשובה שאנחנו זוכרים משבוע שעבר: |
| 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:

|  |
| --- |
| ההודעה שאנחנו מקבלים היא הודעת השגיאה המוכרת שקיבלנו בהתחלה: |
| 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! אם הצלחתם, צרפו צילום מסך והסבירו כיצד מחושב החלק הראשון של ה-Checksum.

|  |
| --- |
| החלק הראשון של הצ'קסאם הוא סכום האותיות באנגלית שנמצאות בשם העיר (a זה 1, b זה 2 וכו') |
| תשובה |