

דוח פרויקט רשתות תקשורת מחשבים - חלק 1

אביטל יוחננוב, נאור אנידג'ר

מבוא

בפרויקט הזה המטרה הייתה לקחת הודעות ברמת אפליקציה, להמיר אותן לפקטות TCP/IP בצורה ידנית ולראות איך הן נראות בפועל בתוך Wireshark. בנוסף היינו צריכים לקשר בין השורות בקובץ ה-CSV לבין הפקטות שנוצרו ונקלטו ברשת.

טעינת קובץ ה-CSV

בשלב הראשון טענו את קובץ ה-CSV המכיל את הודעות האפליקציה המדמות גלישה ברשת (פרוטוקול HTTP), נעזרנו בבינה מלאכותית על מנת לכתוב את הודעות האפליקציה. הטבלה שהתקבלה במחברת הציגה את כל השורות בפורמט הנדרש, כולל השדות:

msg_id, app_protocol, src_app, dst_app, message, timestamp.

Step 1 — Load Your CSV (Input)

1. Place your CSV file (e.g., `group05_http_input.csv`) in the same folder as this notebook.
2. The CSV must contain the following columns: `msg_id`, `app_protocol`, `src_app`, `dst_app`, `message`, `timestamp`.
3. In the next cell, set `CSV_PATH` to your file name and run the cell.
4. Verify that the preview shows your rows correctly.

```
#TODO: Load CSV file with messages into pandas DataFrame,  
  
# Replace 'path_to_your_file.csv' with the actual file path  
import pandas as pd  
filename = r"C:\Users\Avital\Desktop\למודים\רנה בלשימודים\שמות תקשורת מחשבים\groupAvitalNaor_http_input.csv"  
messages_df = pd.read_csv(filename)  
messages_df
```

[4] ✓ 0.0s

Python

	msg_id	app_protocol	src_app	dst_app	message	timestamp
0	1	HTTP	client_browser	web_server	GET /index.html	0.010
1	2	HTTP	web_server	client_browser	200 OK (index.html)	0.018
2	3	HTTP	client_browser	web_server	GET /styles.css	0.026
3	4	HTTP	web_server	client_browser	200 OK (styles.css)	0.034
4	5	HTTP	client_browser	web_server	POST /login username=avital	0.045
5	6	HTTP	web_server	client_browser	302 Redirect /home	0.052
6	7	HTTP	client_browser	web_server	GET /home	0.060
7	8	HTTP	web_server	client_browser	200 OK (home page)	0.072
8	9	HTTP	client_browser	web_server	GET /images/logo.png	0.083
9	10	HTTP	web_server	client_browser	200 OK (logo.png)	0.095
10	11	HTTP	client_browser	web_server	GET /logout	0.110
11	12	HTTP	web_server	client_browser	200 OK Logged out	0.121

בניית מבנה הפקטה (Encapsulation)

הקוד במחברת יוצר באופן ידני את שכבות TCP וIP:

- יצירת TCP Header הכולל source port, destination port, sequence number, flags ועוד.
- יצירת IP Header הכולל כתובות מקור/יעד TTL, Identification, ועוד.
- חיבור הכותרות יחד עם ה-Payload ליצירת פקטה מלאה.

לאחר יצירת הפקטה ניתן היה לראות Hexdump שמציג את המבנה ההקסדצימלי של כל השדות.

```
# Preview packet structure
src_ip = '127.0.0.1'
dst_ip = '127.0.0.1'
src_port = random.randint(1024, 65535)
dst_port = 12345
payload = b'Hello Packet (preview)'
pkt_preview = build_ip_header(src_ip, dst_ip, 20 + len(payload)) + build_tcp_header(src_ip, dst_ip, src_port, dst_port, payload) + payload
hexdump(pkt_preview)
```

[14] ✓ 0.0s Python

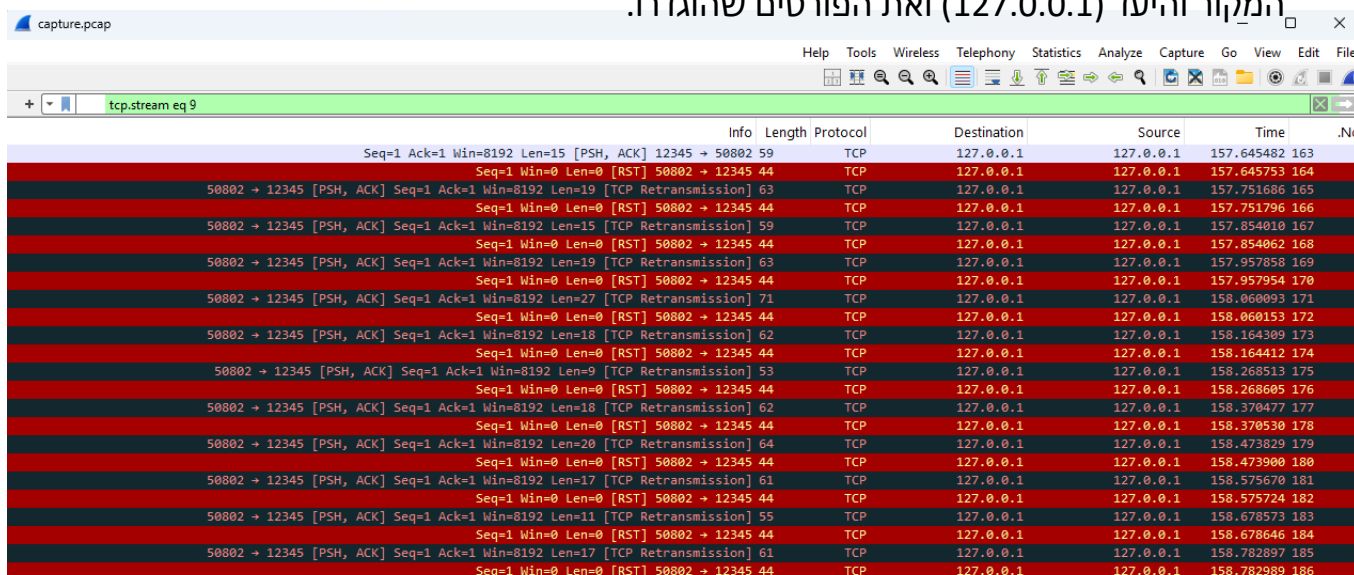
```
... 0000 45 00 00 3e b8 37 00 00 40 06 c4 80 7f 00 00 01 E...>.7..@.....
0010 7f 00 00 01 1c 3a 30 39 79 43 2a 4f 00 00 00 00 .....:09yC*0....
0020 50 02 ff ff ad f1 00 00 48 65 6c 6c 6f 20 50 61 P.....Hello Pa
0030 63 6b 65 74 20 28 70 72 65 76 69 65 77 29 cket (preview)
```

שליחת הפקטות בפועל ולכידה ב-Wireshark

לאחר הכנת הפקטות, ביצענו את שלב השידור והלכידה:

1. הפעלנו את Wireshark והגדרנו האזנה לממשק ה-Loopback (התעבורה הפנימית של המחשב).
2. הרצנו את לולאת השידור במחברת הקוד, שעברה על כל שורות ה-CSV- ושלחה אותן בזז אחר זז לרשת.

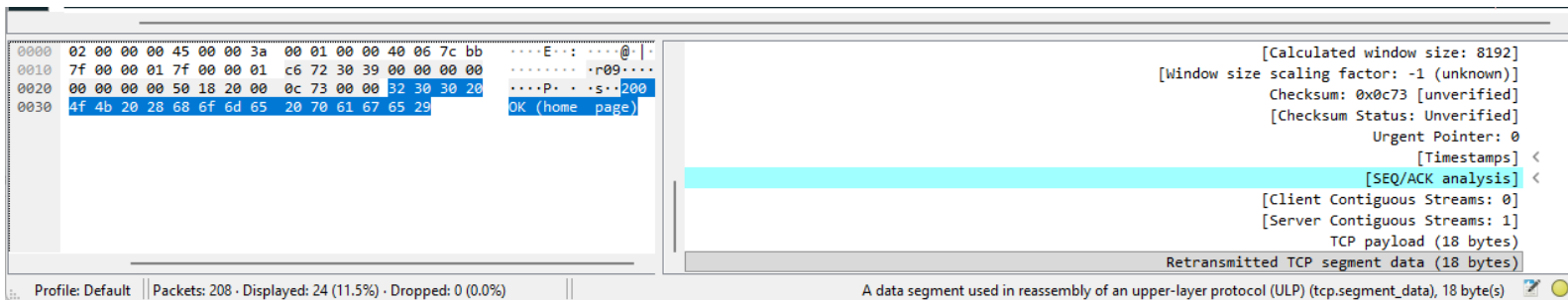
תוצאות הלכידה הראו בבירור את רצף הפקטות שנשלחו. ניתן לראות את כתובות המקור והיעד (127.0.0.1) ואת הפורטים שהוגדרו.



No.	Time	Source	Destination	Protocol	Length	Info
163	157.645482	127.0.0.1	127.0.0.1	TCP	59	Seq=1 Ack=1 Win=8192 Len=15 [PSH, ACK] 12345 → 50802
164	157.645753	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
165	157.751686	127.0.0.1	127.0.0.1	TCP	63	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=19 [TCP Retransmission]
166	157.751796	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
167	157.854010	127.0.0.1	127.0.0.1	TCP	59	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=15 [TCP Retransmission]
168	157.854062	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
169	157.957858	127.0.0.1	127.0.0.1	TCP	63	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=19 [TCP Retransmission]
170	157.957954	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
171	158.060093	127.0.0.1	127.0.0.1	TCP	71	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=27 [TCP Retransmission]
172	158.060153	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
173	158.164309	127.0.0.1	127.0.0.1	TCP	62	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=18 [TCP Retransmission]
174	158.164412	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
175	158.268513	127.0.0.1	127.0.0.1	TCP	53	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=9 [TCP Retransmission]
176	158.268605	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
177	158.370477	127.0.0.1	127.0.0.1	TCP	62	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=18 [TCP Retransmission]
178	158.370530	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
179	158.473829	127.0.0.1	127.0.0.1	TCP	64	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=20 [TCP Retransmission]
180	158.473900	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
181	158.575670	127.0.0.1	127.0.0.1	TCP	61	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=17 [TCP Retransmission]
182	158.575724	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
183	158.678573	127.0.0.1	127.0.0.1	TCP	55	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=11 [TCP Retransmission]
184	158.678646	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345
185	158.782897	127.0.0.1	127.0.0.1	TCP	61	50802 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=17 [TCP Retransmission]
186	158.782989	127.0.0.1	127.0.0.1	TCP	44	Seq=1 Win=0 Len=0 [RST] 50802 → 12345

ניתוח ואימות התוכן (Payload Analysis)

בחרנו באחת הפקטות שנלכדו על מנת לוודא שתוכן ההודעה עבר בצורה תקינה. בחרנו לדוגמא פקטה המכילה בקשת HTTP. בתחתית המסך בחלונית ה-bytes ניתן לראות את הטקסט שנשלח "200 OK (home page)". זה מאשר שתהליך האריזה הידני והשידור עבדו, והמידע עבר משכבת האפליקציה ועד לשכבת הרשת בשלמותו.



קבצים מצורפים להגשה:

- קובץ CSV
- Jupiter Notebook
- pcap