

פרויקט ברשותות תקשורת

מגישים:

ליורי ליבל (212289987)

MICHAEL KANNIN (207973363)

רועי מימן (207972290)

חלק 1: אריזה ולכידת מננות (Encapsulation & Capture)

1. ייצור קובץ הנתונים (CSV)

בשלב הראשון של הפרויקט, נדרשו ליצור תעבורת מדומינית של אפליקציה. לצורך כך, יצרנו קובץ CSV (בשם group212289987_http_input.csv) המכיל רשימה של הודעות בפרוטוקול HTTP, הקובץ נוצר בסיווג כל AI כדי להבטיח פורמט תקין ונתונים מגוונים, והוא כולל את השדות הבאים: מזהה הודעה, פרוטוקול, אפליקציית מקור, אפליקצייתיעד תוכן הודעה וחומרת זמן.

תהליך אריזת המנות(Encapsulation)

באמצעות מחברת Jupyter ביצענו סימולציה ידנית של תהליך הרכimos (Encapsulation) המתרחש במערכת הפעלה:

1. **שכבת היישום (Application):** חילצנו את המידע הגלומי (ההודעה) מתוך ה- CSV.
2. **שכבת התעבורה (Transport):** לכל הודעה הוספנו כותרת (Header) של פרוטוקול TCP/UDP הכוללת את פורט המקור ופורט היעד.
3. **שכבת הרשת (Network):** עטפנו את המגזר בכתובת IP הכוללת את כתובות ה IP-של המקור והיעד.
4. **שידור:** שלחנו את המנות המוכנות דרך משק הרשת, כך שתוכנת Wireshark תוכל ללכוד אותן.

ניתוח לכידת התעבורה(Wireshark)

לאחר הרצת המחברת, ניתן את קובץ הלכידה csv_result.pcap.

דיהוי הפרוטוקול Wireshark: דיהה את המנות TCP/TCP-בהתבסס על ה포רטים שהוגדרו.

תוכן המנה (Payload): בטור גוף המנה, ניתן לראות בבירור את הטעסן שנלקח מקובץ ה- CSV.

תובנה: התרגיל המחייב כיצד כל שכבה מוסיפה את המידע הדרוש לה (Headers) ללא תלות בתוכן המידע עצמו.

לכידת מנתה ה- CSV ב Wireshark

The figure consists of two vertically stacked screenshots of the Wireshark network traffic analyzer. Both screenshots are titled "tcp.port==12345".

Top Screenshot: This screenshot shows a list of captured network frames. Most frames are red, indicating they are RST (Reset) packets. The first few frames are green, showing TCP SYN (Synchronize) and ACK (Acknowledge) packets. The packet details pane shows the following sequence of frames:

```

> Frame 128: Packet, 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 63872, Dst Port: 12345, Seq: 1, Ack: 1, Len: 24
> Data (24 bytes)

```

The bytes pane shows the raw hex and ASCII data for these frames, including the IP header and the TCP header with sequence numbers and acknowledgment numbers.

Bottom Screenshot: This screenshot shows a list of captured network frames. Most frames are red, indicating they are RST (Reset) packets. The first few frames are green, showing TCP SYN (Synchronize) and ACK (Acknowledge) packets. The packet details pane shows the following sequence of frames:

```

> Frame 130: Packet, 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 63672, Dst Port: 12345, Seq: 1, Ack: 1, Len: 15

```

The bytes pane shows the raw hex and ASCII data for these frames, including the IP header and the TCP header with sequence numbers and acknowledgment numbers.

חלק 2: יישום צ'אט וניתוח תעבורת

מבנה המערכת והקוד

פיתחנו מערכת צ'אט מבוססת Sockets ב Python-הפעלת בארכיטקטורת שרת-לקוח-Client-Server (Client-Server). המערכת אינה משתמשת בספריות ניהול שירותים חיצונית, אלא מימושת את התקשרות באמצעות שיר.

רכיבי המערכת:

1. השרת (server.py) :

מנהל את כל התעבורה

ריבוי תהליכי (Multi-threading) עברו כל לקוח שמתחבר, השרת פותח Thread נפרד. מנגנון זה מאפשר לשרת לטפל במספר רב של לקוחות במקביל (מעל 5 כנדרש) מבלי לחסום את התקשרות עם לקוחות אחרים.

השרת מנהל רשימת משתמשים מחוברים ומבצע ניתוב (Routing) של הודעות מלוקוח אחד לאחר.

2. הלקווח (client.py / Gui_Client.py) :

פותח חיבור TCP לשרת ומفرد בין תהליכי השידור והקליטה באמצעות Threads, מה שמאפשר קבלת הודעות בזמן אמת.

ממשק גרפי (GUI) כחלק מבונוס, פיתחנו ממשק משתמש באמצעות ספריית Tkinter המאפשרת למשתמש, מציג את ההיסטוריה הצ'אט ומفرد ויזואלית בין הודעות כניסה ליציאה.

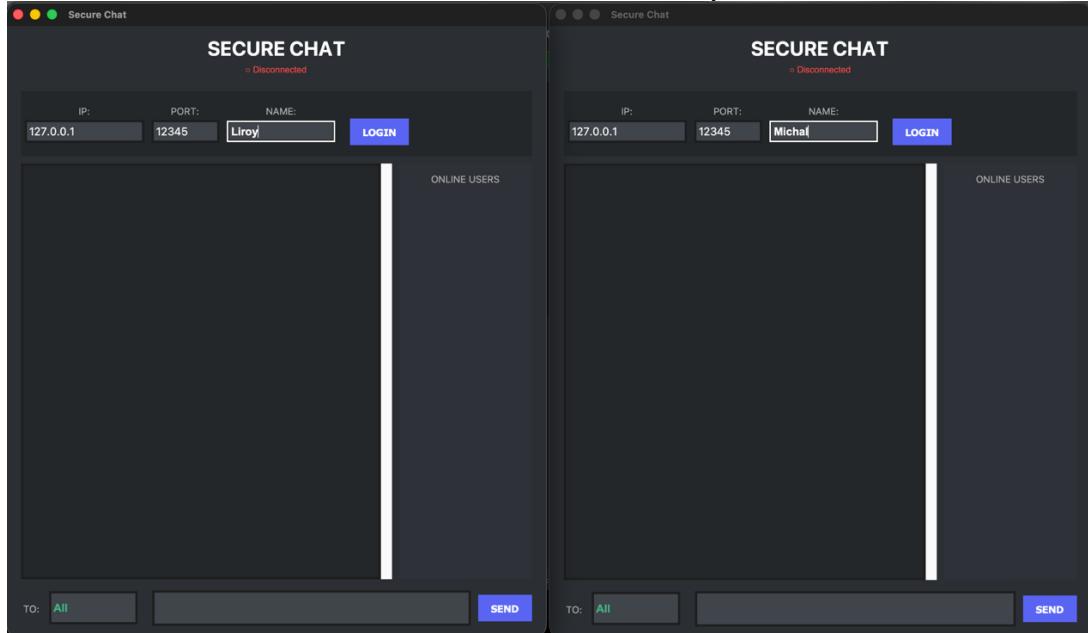
הוראות התקינה והרצתה:

המערכת מtabססת על ספריות סטנדרטיות של Python וAINA דורשת התקנות מיוחדות.

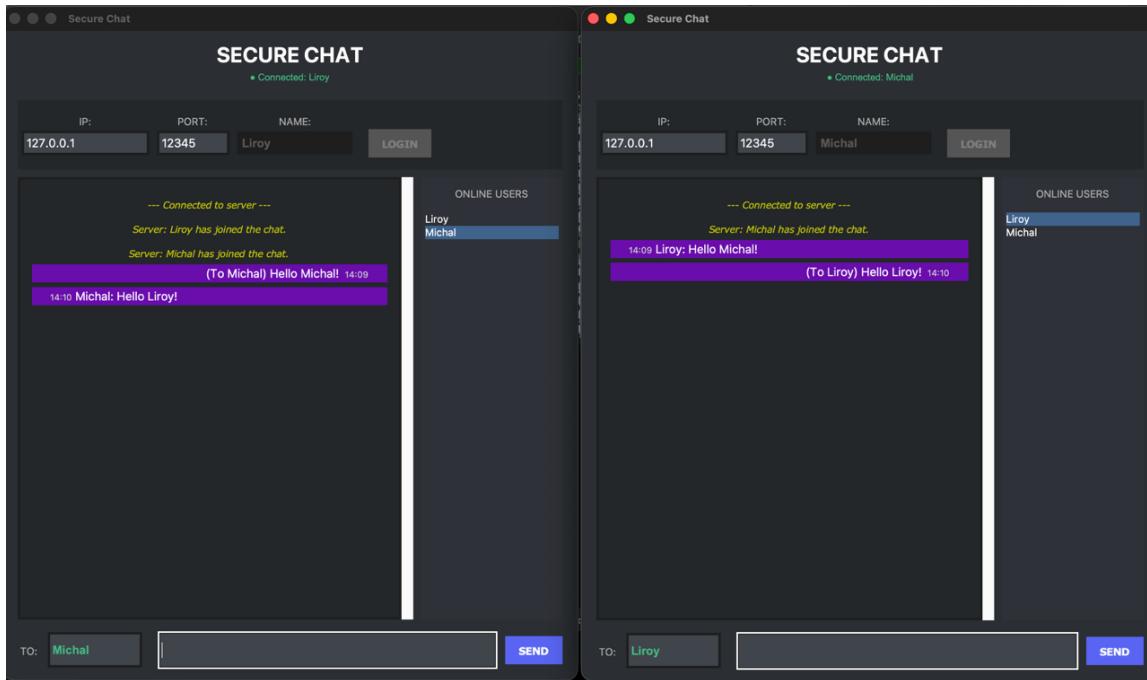
1. יש להפעיל את השרת באמצעות הפקודה python server.py: השרת ידפיס הודעה כי הוא מאזין לחיבורים.
2. עברו כל משתמש, יש להפעיל את הלקווח python Gui_Client.py:
3. בחלון שנפתח, יש להזין שם משתמש ולהתחל בשייחה.

דוגמאות קלט ופלט:

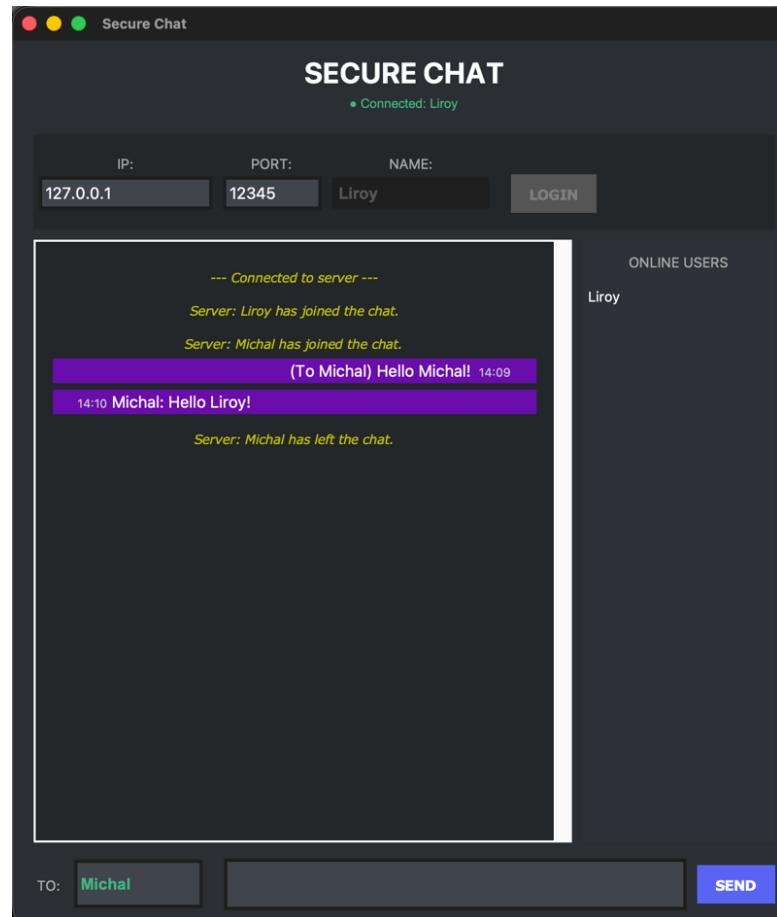
א. ממשק המשתמש (GUI) בתמונה הבאה ניתן לראות את חלון הציג את שפיטחנו. הממשק מאפשר חיבור נוח וצפיה בהודעות בזמן אמת.



ב. תרחיש שיחה בין לקוחות בתרחיש זה הפעילו שני לקוחות במקביל. ההודעה שנשלחה מלקוח א' התקבלה מיידית אצל לקוח ב.'



ג. לוג השרת השירות מציג בזמן אמת את הסטטוס של המחברים והודעות מערכת כולל התראה על עציבה והצטרפות לצ'אט.



ניתוח תעבורת היישום

בניתוח קובץ הילכידה Chat_Analyze.pcap ניתן לראות את שלבי הփוטווקול:TCP

1. יצירת הקשר (Handshake): רואים את תהליך SYN, SYN-ACK, ACK.
2. העברת מידע (Data Transfer): הודעות הצ'אט (כגון שמות המשתמשים והתוכן) מועברות במנוגות עם דגל PSH (Push). מיד לאחר מכן מתקבל אישור ACK.

3. סיום קשר: בעת סגירת החלון, נשלחת מנת FIN/RST לסגירת Socket.

הודעת הצליפות:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|---------------|----------------|----------|--------|---|
| 5 | 128.005320 | 10.100.102.26 | 10.100.102.255 | UDP | 76 | 57621 - 57621 Len=44 |
| 6 | 121.345119 | 127.0.0.1 | 224.0.0.251 | MDNS | 367 | Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question |
| 7 | 121.345305 | fe80::1 | ff02::fb | MDNS | 387 | Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question |
| 8 | 121.345386 | 10.100.102.26 | 224.0.0.251 | MDNS | 367 | Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question |
| 9 | 121.345471 | fe80::1 | ff02::fb | MDNS | 387 | Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question |
| 10 | 136.378115 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 61018 - 12345 [SYN] Seq=0 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=1373009323 Tsec=0 SACK_PERM |
| 11 | 136.378254 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 12345 - 61018 [SYN, ACK] Seq=1 Ack=1 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=1464157686 Tsec=137300932 |
| 12 | 136.378284 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 - 12345 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=1464157686 Tsec=137300932 |
| 13 | 136.378302 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | [TCP Window Update] 12345 - 61018 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=1464157686 Tsec=137300932 |
| 14 | 136.378327 | 127.0.0.1 | 127.0.0.1 | TCP | 61 | 61018 - 12345 [PSH, ACK] Seq=1 Ack=1 Win=408320 Len=5 Tsvl=1373009323 Tsec=1464157686 |
| 15 | 136.378345 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61018 [ACK] Seq=1 Ack=1 Win=408320 Len=5 Tsvl=1373009323 Tsec=1464157686 |
| 16 | 136.378979 | 127.0.0.1 | 127.0.0.1 | TCP | 91 | 91 12345 - 61018 [PSH, ACK] Seq=1 Ack=6 Win=408320 Len=35 Tsvl=1464157686 Tsec=1373009323 |
| 17 | 136.379013 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 - 12345 [ACK] Seq=6 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157686 |
| 18 | 136.379031 | 127.0.0.1 | 127.0.0.1 | TCP | 73 | 61018 - 12345 [SYN, ACK] Seq=3 Win=6 Win=408320 Len=17 Tsvl=1464157687 Tsec=1373009324 |
| 19 | 136.379035 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61018 [ACK] Seq=0 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157687 |
| 20 | 137.491667 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 61019 - 12345 [SYN] Seq=0 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=365444783 Tsec=0 SACK_PERM |
| 21 | 137.491753 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61019 [SYN, ACK] Seq=0 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=1036117598 Tsec=365444783 |
| 22 | 137.491776 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | [TCP Window Update] 12345 - 61019 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=365444783 Tsec=1036117598 |
| 23 | 137.491786 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 - 12345 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=1036117598 Tsec=365444783 |
| 24 | 137.491798 | 127.0.0.1 | 127.0.0.1 | TCP | 62 | 61019 - 12345 [PSH, ACK] Seq=1 Ack=1 Win=408320 Len=5 Tsvl=365444783 Tsec=1036117598 |
| 25 | 137.491816 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61019 [ACK] Seq=1 Ack=1 Win=408320 Len=5 Tsvl=1036117598 Tsec=365444783 |
| 26 | 137.491966 | 127.0.0.1 | 127.0.0.1 | TCP | 92 | 92 12345 - 61018 [PSH, ACK] Seq=53 Ack=6 Win=408320 Len=36 Tsvl=1464157686 Tsec=1373009324 |
| 27 | 137.491974 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 - 12345 [ACK] Seq=6 Win=408320 Len=36 Tsvl=1036117591 Tsec=365444783 |
| 28 | 137.491985 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61018 [ACK] Seq=6 Win=408320 Len=6 Tsvl=1373010437 Tsec=1464158799 |
| 29 | 137.491991 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 - 12345 [ACK] Seq=7 Ack=37 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157687 |
| 30 | 137.491997 | 127.0.0.1 | 127.0.0.1 | TCP | 88 | 12345 - 61018 [PSH, ACK] Seq=99 Ack=6 Win=408320 Len=24 Tsvl=1464158800 Tsec=1373010437 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------------|-------------|----------|--------|---|
| 9 | 121.345471 | 108:01:87:61:26:65.. | 110:01:17:6 | MDNS | 367 | Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question |
| 10 | 136.378115 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 61018 - 12345 [SYN] Seq=0 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=1373009323 Tsec=0 SACK_PERM |
| 11 | 136.378254 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 12345 - 61018 [SYN, ACK] Seq=1 Ack=1 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=1464157686 Tsec=137300932 |
| 12 | 136.378284 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 - 12345 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=1373009323 Tsec=1464157686 |
| 13 | 136.378302 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | [TCP Window Update] 12345 - 61018 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=1373009323 Tsec=1464157686 |
| 14 | 136.378327 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 - 12345 [PSH, ACK] Seq=1 Ack=1 Win=408320 Len=5 Tsvl=1373009323 Tsec=1464157686 |
| 15 | 136.378345 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61018 [ACK] Seq=1 Ack=1 Win=408320 Len=5 Tsvl=1373009323 Tsec=1464157686 |
| 16 | 136.378979 | 127.0.0.1 | 127.0.0.1 | TCP | 91 | 91 12345 - 61018 [PSH, ACK] Seq=1 Ack=6 Win=408320 Len=35 Tsvl=1464157686 Tsec=1373009323 |
| 17 | 136.379013 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 - 12345 [ACK] Seq=6 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157686 |
| 18 | 136.379031 | 127.0.0.1 | 127.0.0.1 | TCP | 73 | 61018 - 12345 [SYN, ACK] Seq=3 Win=6 Win=408320 Len=17 Tsvl=1464157687 Tsec=1373009324 |
| 19 | 136.379035 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61018 [ACK] Seq=0 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157687 |
| 20 | 137.491667 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 61019 - 12345 [SYN] Seq=0 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=365444783 Tsec=0 SACK_PERM |
| 21 | 137.491753 | 127.0.0.1 | 127.0.0.1 | TCP | 68 | 12345 - 61019 [SYN, ACK] Seq=0 Win=65535 Len=64 MSS=16344 WS=64 Tsvl=1036117598 Tsec=365444783 |
| 22 | 137.491776 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 - 12345 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=365444783 Tsec=1036117598 |
| 23 | 137.491786 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | [TCP Window Update] 12345 - 61019 [ACK] Seq=1 Ack=1 Win=408320 Len=0 Tsvl=365444783 Tsec=1036117598 |
| 24 | 137.491798 | 127.0.0.1 | 127.0.0.1 | TCP | 62 | 61019 - 12345 [PSH, ACK] Seq=1 Ack=1 Win=408320 Len=6 Tsvl=365444783 Tsec=1036117598 |
| 25 | 137.491816 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61019 [ACK] Seq=6 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157687 |
| 26 | 137.491966 | 127.0.0.1 | 127.0.0.1 | TCP | 92 | 92 12345 - 61019 [PSH, ACK] Seq=53 Ack=6 Win=408320 Len=36 Tsvl=1464157686 Tsec=1373009324 |
| 27 | 137.491974 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 - 12345 [ACK] Seq=6 Win=408320 Len=36 Tsvl=1036117591 Tsec=365444783 |
| 28 | 137.491985 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 - 61019 [ACK] Seq=6 Win=408320 Len=6 Tsvl=1373010437 Tsec=1464158799 |
| 29 | 137.491991 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 - 12345 [ACK] Seq=7 Ack=37 Win=408320 Len=0 Tsvl=1373009324 Tsec=1464157687 |
| 30 | 137.491997 | 127.0.0.1 | 127.0.0.1 | TCP | 88 | 12345 - 61019 [PSH, ACK] Seq=99 Ack=6 Win=408320 Len=24 Tsvl=1464158800 Tsec=1373010437 |

Bytes 56-91: Data (data)

Packets: 56 Profile: Default

הודעות בין משתמשים:

| No. | Time | Source | Destination | Protocol | Length | Info |
|--|--------------|---------------|----------------|----------|--|---|
| 33 | 137.492006 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=7 Ack=61 Win=408320 Len=0 TSval=3654447484 TSecr=1036117591 |
| 34 | 150.007138 | 10.100.102.26 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 35 | 160.409390 | 127.0.0.1 | 127.0.0.1 | TCP | 76 | 61018 → 12345 [PSH, ACK] Seq=9 Ack=113 Win=408320 Len=20 TSval=1373033355 TSecr=1464158800 |
| 36 | 160.409455 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=113 Ack=26 Win=408320 Len=0 TSval=1464181717 TSecr=1373033354 |
| 37 | 160.409574 | 127.0.0.1 | 127.0.0.1 | TCP | 87 | 12345 → 61019 [PSH, ACK] Seq=61 Ack=7 Win=408320 Len=31 TSval=1036140508 TSecr=3654444784 |
| 38 | 160.409598 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=7 Ack=92 Win=408320 Len=0 TSval=36544467701 TSecr=1036140508 |
| 39 | 172.762773 | 127.0.0.1 | 127.0.0.1 | TCP | 74 | 61019 → 12345 [PSH, ACK] Seq=7 Ack=92 Win=408320 Len=18 TSval=3654480054 TSecr=1036140508 |
| 40 | 172.762840 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=92 Ack=25 Win=408320 Len=0 TSval=1036152861 TSecr=3654480054 |
| 41 | 172.762941 | 127.0.0.1 | 127.0.0.1 | TCP | 87 | 12345 → 61018 [PSH, ACK] Seq=113 Ack=26 Win=408320 Len=31 TSval=1464194071 TSecr=1373033354 |
| 42 | 172.762962 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=144 Win=408320 Len=0 TSval=1373045708 TSecr=1464194071 |
| 43 | 180.007962 | 10.100.102.26 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 44 | 186.297389 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [PSH, ACK] Seq=25 Ack=92 Win=408320 Len=0 TSval=3654493589 TSecr=1036152861 |
| 45 | 186.297373 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=92 Ack=26 Win=408320 Len=0 TSval=1036166396 TSecr=3654493589 |
| 46 | 186.297587 | 127.0.0.1 | 127.0.0.1 | TCP | 98 | 12345 → 61018 [PSH, ACK] Seq=144 Ack=26 Win=408320 Len=34 TSval=1464207605 TSecr=1373045708 |
| 47 | 186.297617 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=178 Win=408320 Len=0 TSval=1373059242 TSecr=1464207605 |
| 48 | 186.297632 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [FIN, ACK] Seq=92 Ack=26 Win=408320 Len=0 TSval=1036166396 TSecr=3654493589 |
| 49 | 186.297639 | 127.0.0.1 | 127.0.0.1 | TCP | 73 | 12345 → 61018 [PSH, ACK] Seq=178 Ack=26 Win=408320 Len=17 TSval=1464207605 TSecr=1373059242 |
| 50 | 186.297666 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=26 Ack=93 Win=408320 Len=0 TSval=3654493589 TSecr=1036166396 |
| 51 | 186.297670 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=195 Win=408320 Len=0 TSval=1373059242 TSecr=1464207605 |
| 52 | 210.008868 | 10.100.102.26 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 53 | 215.846177 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [FIN, ACK] Seq=26 Ack=195 Win=408320 Len=0 TSval=1373088791 TSecr=1464207605 |
| 54 | 215.846246 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [ACK] Seq=195 Ack=27 Win=408320 Len=0 TSval=1464237154 TSecr=1373088791 |
| > Frame 41: Packet, 87 bytes on wire (696 bits), 87 bytes captured (696 bits) | | | | | 0000 02 00 00 00 45 00 00 53 00 00 40 00 40 06 00 00 | ... E-S -@... |
| > Null/Loopback | | | | | 0010 ff 00 00 01 7f 00 00 01 30 39 ee 50 8c 6b eb | ... 9. k... |
| > Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 | | | | | 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ... R... G... |
| > Transmission Control Protocol, Src Port: 12345, Dst Port: 61018, Seq: 113, Ack: 26, Len: 3 | | | | | 0030 57 45 d4 17 51 d6 d3 8a 28 50 72 69 76 61 74 65 | WE_Q... (Private |
| > Data (31 bytes) | | | | | 0040 29 20 4d 69 63 68 61 6c 3a 20 48 65 6c 6c 6f 20 |) Michal: Hello |
| Data: 28507269766174652904d696368616c3a2048656c6c6f204c69726f79210a | [Length: 31] | | | | 0050 4c 69 72 fd 79 21 0a | Liroy! |

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|--------------|---------------|----------------|----------|--|---|
| 29 | 137.491991 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=9 Ack=65 Win=408320 Len=0 TSval=1373010437 TSecr=1464158800 |
| 30 | 137.491997 | 127.0.0.1 | 127.0.0.1 | TCP | 80 | 12345 → 61018 [PSH, ACK] Seq=89 Ack=66 Win=408320 Len=24 TSval=1464158800 TSecr=1036117591 |
| 31 | 137.492001 | 127.0.0.1 | 127.0.0.1 | TCP | 80 | 12345 → 61019 [PSH, ACK] Seq=37 Ack=7 Win=408320 Len=24 TSval=1036117591 TSecr=3654444784 |
| 32 | 137.492006 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=6 Ack=113 Win=408320 Len=0 TSval=1373018437 TSecr=1464158800 |
| 33 | 137.492006 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=7 Ack=61 Win=408320 Len=0 TSval=3654447484 TSecr=1036117591 |
| 34 | 150.007138 | 10.100.102.26 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 35 | 160.409390 | 127.0.0.1 | 127.0.0.1 | TCP | 76 | 61018 → 12345 [PSH, ACK] Seq=6 Ack=113 Win=408320 Len=20 TSval=1373033354 TSecr=1464158800 |
| 36 | 160.409455 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [ACK] Seq=113 Ack=26 Win=408320 Len=0 TSval=1464181717 TSecr=1373033354 |
| 37 | 160.409574 | 127.0.0.1 | 127.0.0.1 | TCP | 87 | 12345 → 61019 [PSH, ACK] Seq=61 Ack=7 Win=408320 Len=31 TSval=1036140508 TSecr=3654444784 |
| 38 | 160.409598 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=92 Win=408320 Len=0 TSval=3654467701 TSecr=1036140508 |
| 39 | 160.409673 | 127.0.0.1 | 127.0.0.1 | TCP | 74 | 61019 → 12345 [PSH, ACK] Seq=92 Ack=69 Win=408320 Len=18 TSval=3654480054 TSecr=1036140508 |
| 40 | 172.762840 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=92 Ack=25 Win=408320 Len=0 TSval=1036152861 TSecr=3654480054 |
| 41 | 172.762941 | 127.0.0.1 | 127.0.0.1 | TCP | 87 | 12345 → 61018 [PSH, ACK] Seq=113 Ack=26 Win=408320 Len=31 TSval=1464194071 TSecr=1373033354 |
| 42 | 172.762962 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=144 Win=408320 Len=0 TSval=1373045708 TSecr=1464194071 |
| 43 | 180.007962 | 10.100.102.26 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 44 | 186.297389 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [FIN, ACK] Seq=25 Ack=92 Win=408320 Len=0 TSval=3654493589 TSecr=1036152861 |
| 45 | 186.297373 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=92 Ack=26 Win=408320 Len=0 TSval=1373045708 TSecr=1464207605 |
| 46 | 186.297587 | 127.0.0.1 | 127.0.0.1 | TCP | 98 | 12345 → 61018 [PSH, ACK] Seq=144 Ack=26 Win=408320 Len=34 TSval=1464207605 TSecr=1373045708 |
| 47 | 186.297617 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=178 Win=408320 Len=0 TSval=1373059242 TSecr=1464207605 |
| 48 | 186.297632 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [FIN, ACK] Seq=92 Ack=26 Win=408320 Len=0 TSval=1036166396 TSecr=3654493589 |
| 49 | 186.297639 | 127.0.0.1 | 127.0.0.1 | TCP | 73 | 12345 → 61018 [ACK] Seq=178 Ack=26 Win=408320 Len=17 TSval=1464207605 TSecr=1373059242 |
| > Frame 37: Packet, 87 bytes on wire (696 bits), 87 bytes captured (696 bits) | | | | | 0000 02 00 00 00 45 00 00 53 00 00 40 00 40 06 00 00 | ... E-S -@... |
| > Null/Loopback | | | | | 0010 ff 00 00 01 7f 00 00 01 30 39 ee 50 8c 6b eb | ... 9. k... |
| > Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 | | | | | 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ... R... G... |
| > Transmission Control Protocol, Src Port: 12345, Dst Port: 61019, Seq: 61, Ack: 7, Len: 31 | | | | | 0030 c4 b6 36 c4 80 18 18 ec fe 47 00 00 01 00 00 | = 6... G... |
| > Data (31 bytes) | | | | | 0040 3d c2 3f dc d9 62 66 f0 28 50 72 69 76 61 74 65 | = ?-f. (Private |
| Data: 28507269766174652904d696368616c3a2048656c6c6f204c69726f79210a | [Length: 31] | | | | 0050 69 63 68 61 6c 21 0a |) Liroy: Hello M |
| > | | | | | | ichall! |

הודעת עזיבת משתמש מהצ'אט:

Apply a display filter ... <幫/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|---|
| 35 | 160.409398 | 127.0.0.1 | 127.0.0.1 | TCP | 76 | 61018 → 12345 [PSH, ACK] Seq=6 Ack=113 Win=408320 Len=20 TSval=1373033354 TSecr=1464158800 |
| 36 | 160.409455 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [ACK] Seq=113 Ack=26 Win=408320 Len=0 TSval=1464181717 TSecr=1373033354 |
| 37 | 160.409574 | 127.0.0.1 | 127.0.0.1 | TCP | 87 | 12345 → 61019 [PSH, ACK] Seq=61 Ack=7 Win=408320 Len=31 TSval=1036140508 TSecr=3654444784 |
| 38 | 160.409598 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=7 Ack=92 Win=408320 Len=0 TSval=3654467701 TSecr=1036140508 |
| 39 | 172.762773 | 127.0.0.1 | 127.0.0.1 | TCP | 74 | 61019 → 12345 [PSH, ACK] Seq=7 Ack=92 Win=408320 Len=18 TSval=3654480054 TSecr=1036140508 |
| 40 | 172.762840 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=92 Ack=25 Win=408320 Len=0 TSval=1036152861 TSecr=3654480054 |
| 41 | 172.762941 | 127.0.0.1 | 127.0.0.1 | TCP | 87 | 12345 → 61018 [PSH, ACK] Seq=113 Ack=26 Win=408320 Len=31 TSval=1464194071 TSecr=1373033354 |
| 42 | 172.762963 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=144 Win=408320 Len=0 TSval=1373045708 TSecr=1464194071 |
| 43 | 180.007962 | 10.100.102.255 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 44 | 186.297309 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [FIN, ACK] Seq=25 Ack=92 Win=408320 Len=0 TSval=3654493589 TSecr=1036152861 |
| 45 | 186.297373 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [ACK] Seq=92 Ack=26 Win=408320 Len=0 TSval=1036166396 TSecr=3654493589 |
| 46 | 186.297587 | 127.0.0.1 | 127.0.0.1 | TCP | 90 | 12345 → 61018 [PSH, ACK] Seq=144 Ack=26 Win=408320 Len=34 TSval=1464207605 TSecr=1373045708 |
| 47 | 186.297617 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=178 Win=408320 Len=0 TSval=1373059242 TSecr=1464207605 |
| 48 | 186.297632 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61019 [FIN, ACK] Seq=92 Ack=26 Win=408320 Len=0 TSval=1036166396 TSecr=3654493589 |
| 49 | 186.297639 | 127.0.0.1 | 127.0.0.1 | TCP | 73 | 12345 → 61018 [PSH, ACK] Seq=178 Ack=26 Win=408320 Len=17 TSval=1464207605 TSecr=1373059242 |
| 50 | 186.297666 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61019 → 12345 [ACK] Seq=26 Ack=93 Win=408320 Len=0 TSval=3654493589 TSecr=1036166396 |
| 51 | 186.297670 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=26 Ack=195 Win=408320 Len=0 TSval=1373059242 TSecr=1464207605 |
| 52 | 210.008866 | 10.100.102.255 | 10.100.102.255 | UDP | 76 | 57621 → 57621 Len=44 |
| 53 | 215.846177 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [FIN, ACK] Seq=26 Ack=195 Win=408320 Len=0 TSval=1373088791 TSecr=1464207605 |
| 54 | 215.846246 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [ACK] Seq=195 Ack=27 Win=408320 Len=0 TSval=1464237154 TSecr=1373088791 |
| 55 | 215.846482 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 12345 → 61018 [FIN, ACK] Seq=195 Ack=27 Win=408320 Len=0 TSval=1464237154 TSecr=1373088791 |
| 56 | 215.846537 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 61018 → 12345 [ACK] Seq=27 Ack=196 Win=408320 Len=0 TSval=1373088791 TSecr=1464237154 |

```
> Frame 46: Packet, 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 12345, Dst Port: 61018, Seq: 144, Ack: 26, Len: 3
Data: 5365727665723a204d696368616c20686173206c6566742074686520636861742e0a
[Length: 34]
```

0000 02 00 00 00 45 00 00 56 00 00 40 00 40 00 00 00 E· V ·@ @ ··
0010 7f 00 00 01 7f 00 00 01 30 39 ee 5a 8c 6b ec 05 ··· 09 Z k ··
0020 fb b3 03 48 80 18 18 ec fe 4a 00 00 01 01 08 0a ··· H ··· J ···
0030 57 46 08 f5 51 d7 03 cc 53 65 72 76 65 72 3a 20 WF · 0 ··· Server:
0040 4d 69 63 68 61 6c 20 68 61 73 20 6c 65 66 74 20 Michal h as left
0050 74 68 65 20 63 68 61 74 2e 0a the chat ..

Data (data.data), 34 bytes

Packets: 56

Profile: Default

חלק 3: שימוש בביינה מלאכותית (AI)

במסגרת העבודה נעשה שימוש בכל'י הבינה המלאכותית Google Gemini ככלי עזר לפיתוח ולמידה. השימוש בוצע באופן מבוקר תוך בדיקת התוצאות.

מטרות השימוש ודוגמאות לפורמפסיטים:

1. **יצירת נתונים (חלק 1):** (יצירת קובץ CSV-עם נתונים דמה ריאליים לשימולציה).

Prompt Example: "Create a CSV file with columns: msg_id, app_protocol, src_app, dst_app, message, timestamp. Generate 10 rows representing HTTP GET requests."

2. **פיתוח השירות (Server):** סיעע בכתיבה שלד הקוד לטיפול בריבוי לקוחות.(Multi-threading)

Prompt Example: "Write a Python TCP server using 'socket' and 'threading' to handle multiple clients simultaneously."

3. **עיצוב הממשק (GUI):** עזרה בבניית הממשק הגרפי ב Tkinter-וסידור האלמנטים בחלון.

Prompt Example: "Create a GUI chat client in Python using tkinter with a scrollable text area and an input field"