

רשתות תקשורת מחשבים

תרגיל בית 1-חלק wireshark

עלי ריאן 212153266

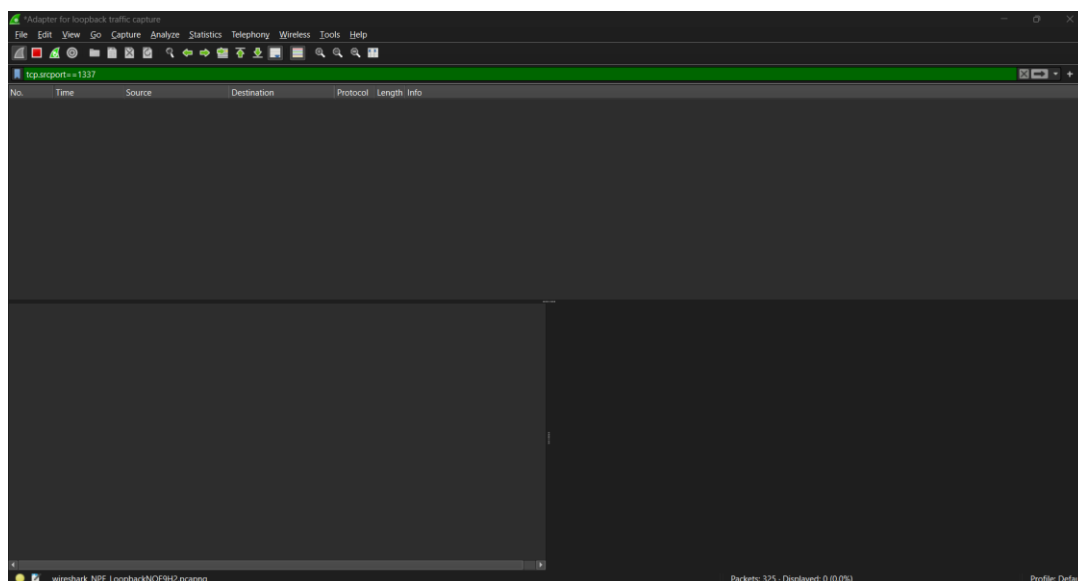
עודי אגבאריה 212609440

תמונות מהwireshark:

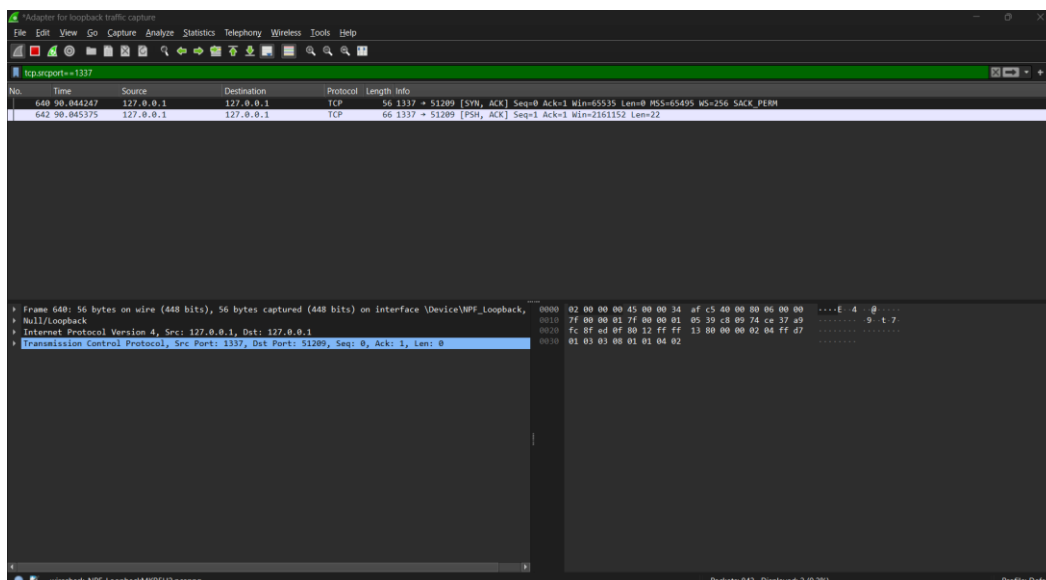
הערה: שמתי שתי תמונות מתחת לכל שלב, התמונה הראשונה היא המקורית אבל לא הצבענו לפקטה המתאימה, לכן הוספנו את התמונה השנייה מהקובץ שנגיש pcap והצבענו על הפקטה המתאימה.

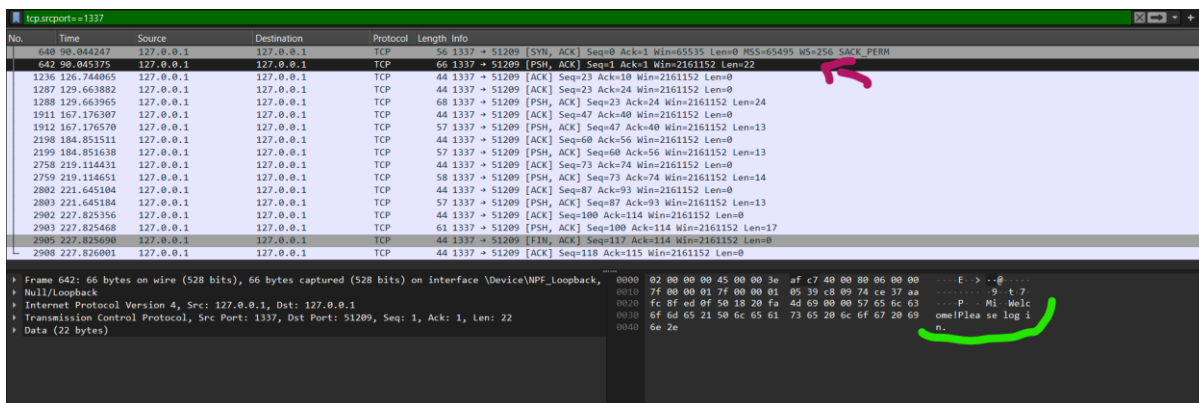
הפילטר נעשה ע"י tcp.srcport=1337

לפני שעשינו connect:

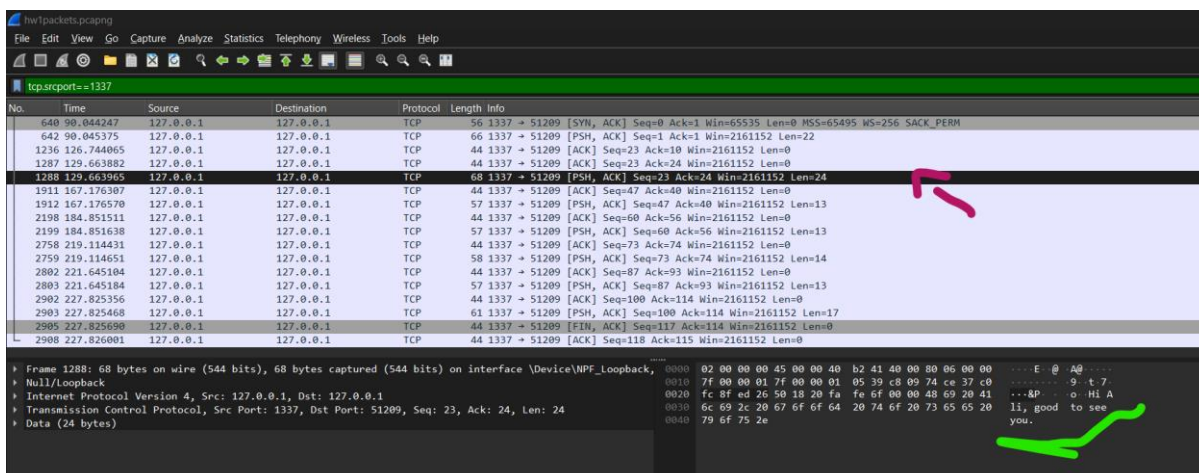
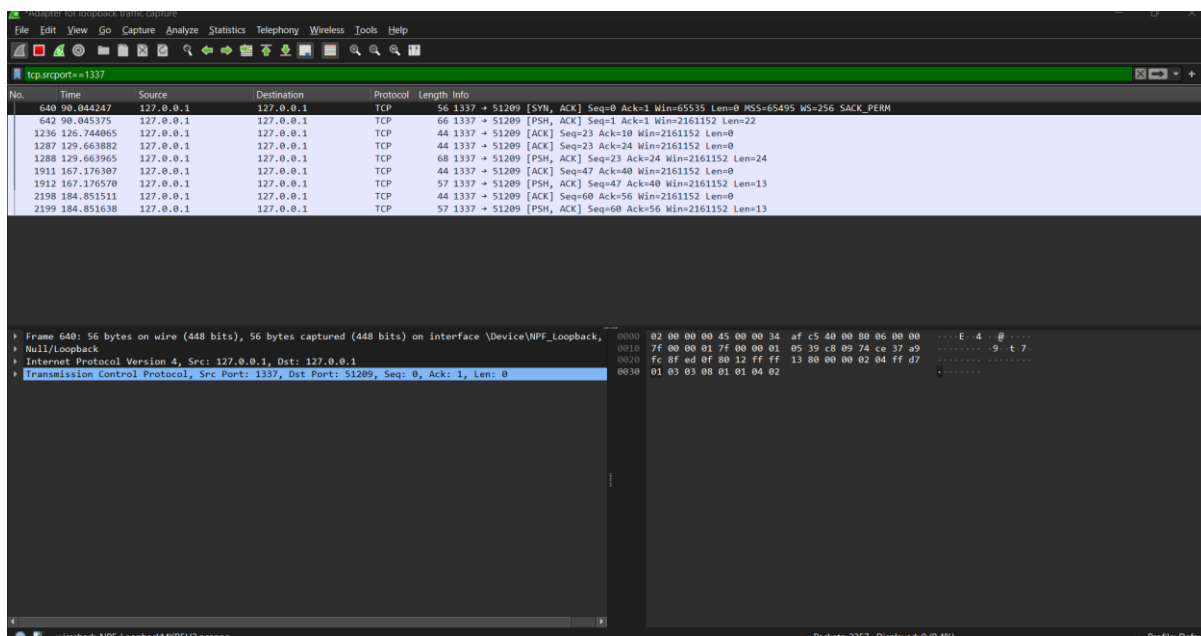


בהתחלה נוכל לראות שאין אף פקטה ב port=1337 עוד לא הופעל השרת.  
אחרי connect:





בשלב זה נוכל לראות שאחרי שהופעל השרת הופיעו פקטות חדשות ונוכל לראות את המקור שלהם שהוא 127.0.0.1 והיעד שלהם הוא גם 127.0.0.1, נוכל לראות גם שהפרוטוקול הוא TCP. בתחתית התמונה מופיעה ההודעה שהיא כתובה בפרוטוקול dns ו http, וכיוון שזה הזמן שהלוקוס נדרש להקיש שם משתמש וסיסמה אכן מופיעה ההודעה המתאימה לשלב הזה שהיא "Welcome! Please log in" הודעה זו שלח השרת ללוקוס. ➤ אחרי ההתחברות (log in):



ניתן לראות את הודעת: "Hi Ali, good to see you" בתחתית התמונה.

## אחרי שליחת שאילתות: ➤

Wireshark capture showing a successful TCP connection establishment. The packet list shows a SYN packet (No. 640) and its corresponding ACK (No. 1236). The packet details pane shows the TCP header with Seq=0, Ack=1, and Win=65535. The packet bytes pane shows the raw data.

Wireshark capture showing a failed TCP connection attempt. The packet list shows a SYN packet (No. 2759) and its corresponding ACK (No. 2802). The packet details pane shows the TCP header with Seq=73, Ack=74, and Win=2161152. The packet bytes pane shows the raw data, with a red arrow pointing to the 'on: Ye s...' text.

פקטה זו נשלחה מהשרת ללקוח אחרי שהלקוח שאלה שאילתה ואז רואים את התגובה של השרת בתחתית בתמונה .