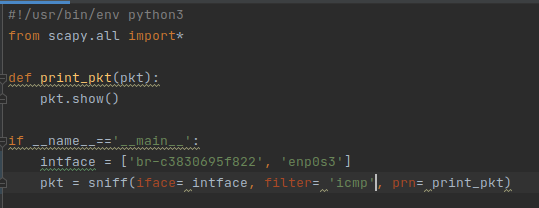
ב"ה

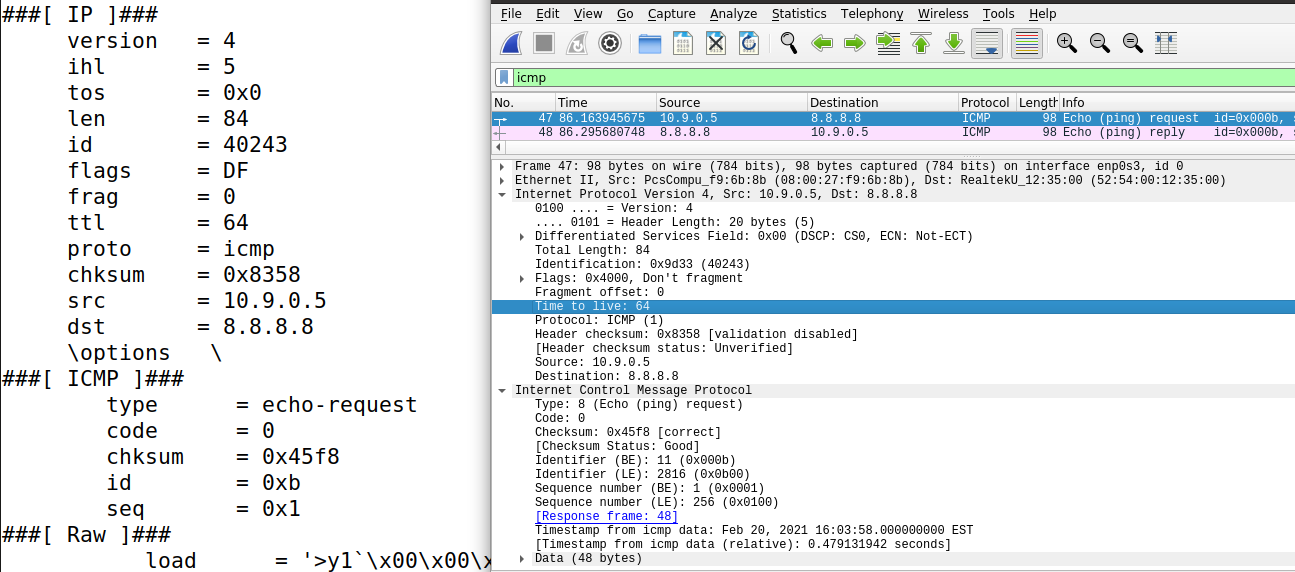
פרויקט גמר בתקשורת

משימה 1.1:

חלק A:

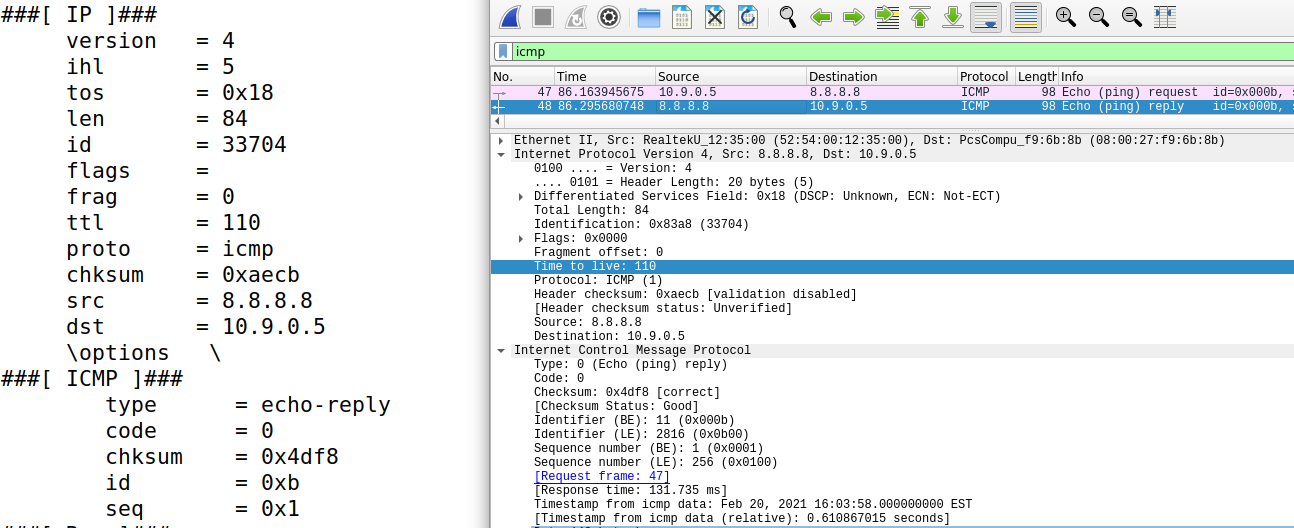
כאן התבקשנו לבנות סניפר בפייתון, ולפלטר לפי icmp. להלן הקוד:

ניתן לראות את תוצאת ההרצה של הקובץ עם הרשאת גישה (sudo), וניתן לראות שהיא זהה לפאקטות שאנו רואים בwireshark:

request:

wireshark

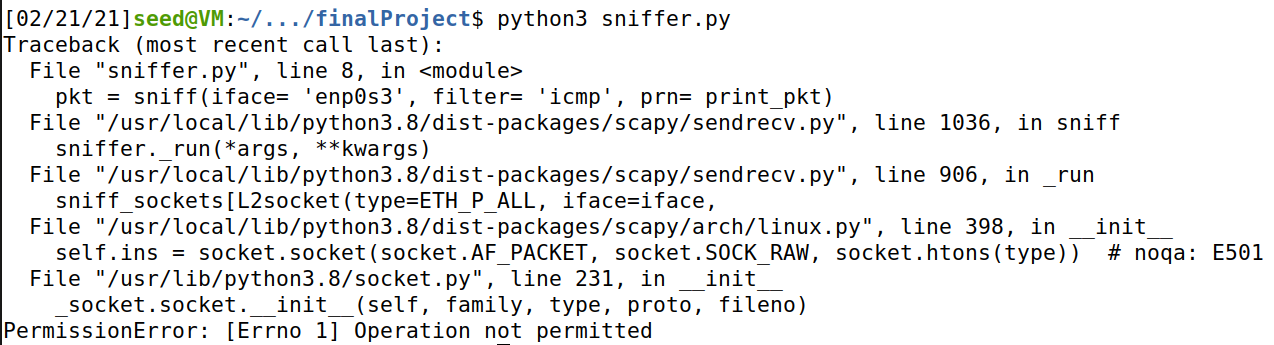
terminal

Reply:

wireshark

terminal

כאן ניתן לראות את תוצאת ההרצה של הקובץ בלי הרשאת גישה (sudo). הסיבה שמתקבלת שגיאה, כי האזנה לפקטות זה דבר שדורש הרשאת מנהל. בלי sudo אין הרשאת מנהל, ולכן לא ניתן להפעיל ,raw socket ולכן מתקבלת שגיאה.

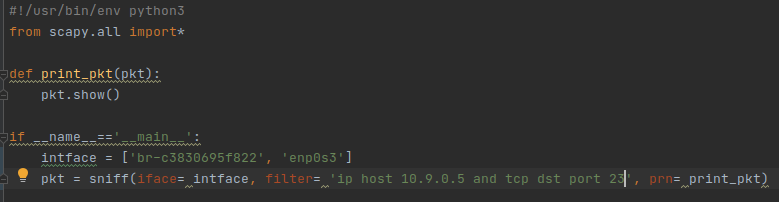
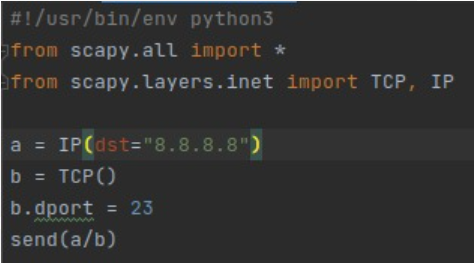


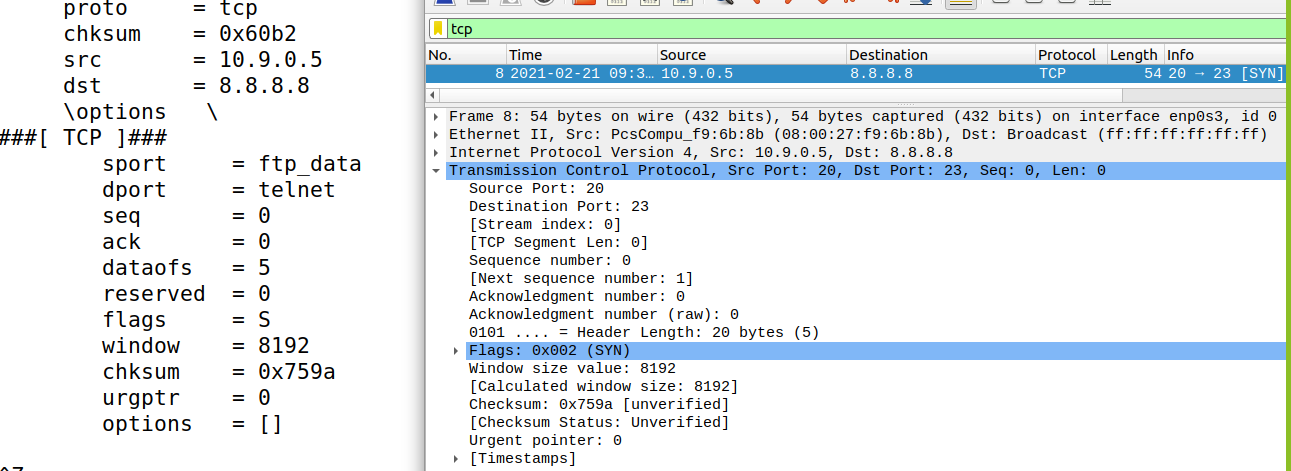
חלק B:

בחלק הזה נתבקשנו לפלטר את הסניפר שבנינו לפי סוגי פקטות:

-לפי icmp: ניתן לראות זאת בתמונה בחלק A, שם הפילטר כבר מסונן לפי icmp

-לפי TCP: כאן אנו מפלטרים פקטות TCP עם פורט יעד 23 עבור IP מסוים (8.8.8.8):

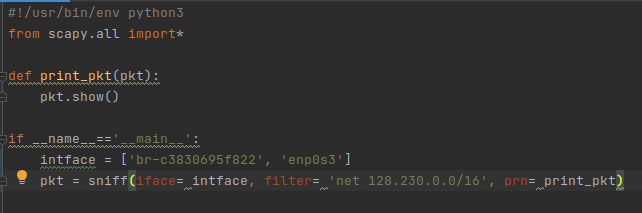
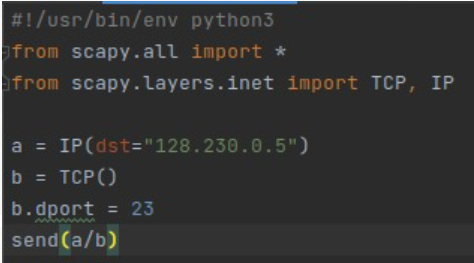
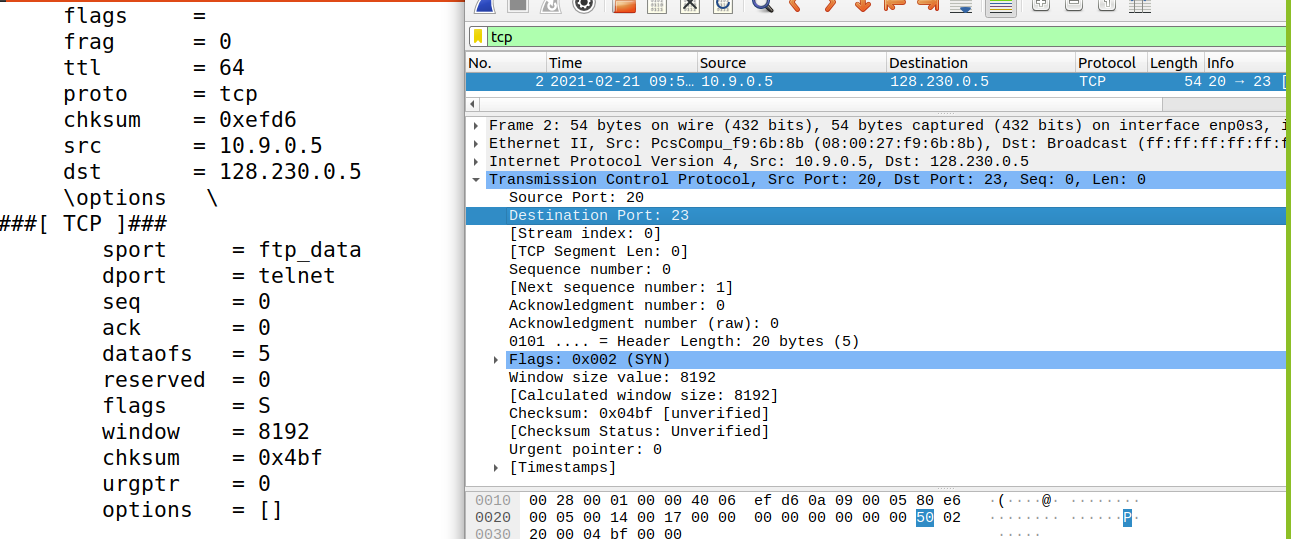


וכאן ניתן לראות שקיבלנו אותן פקטת TCP בטרמינל ובווירשארק:

wireshark

terminal

-כאן נתבקשנו ללכוד פקטות שרצות ברשת פנימית מסוימת (128.230.0.0/16):

כאן ניתן לראות שקיבלנו תוצאה זהה בטרמינל ובווירשארק:

wireshark

terminal

משימה 1.2: