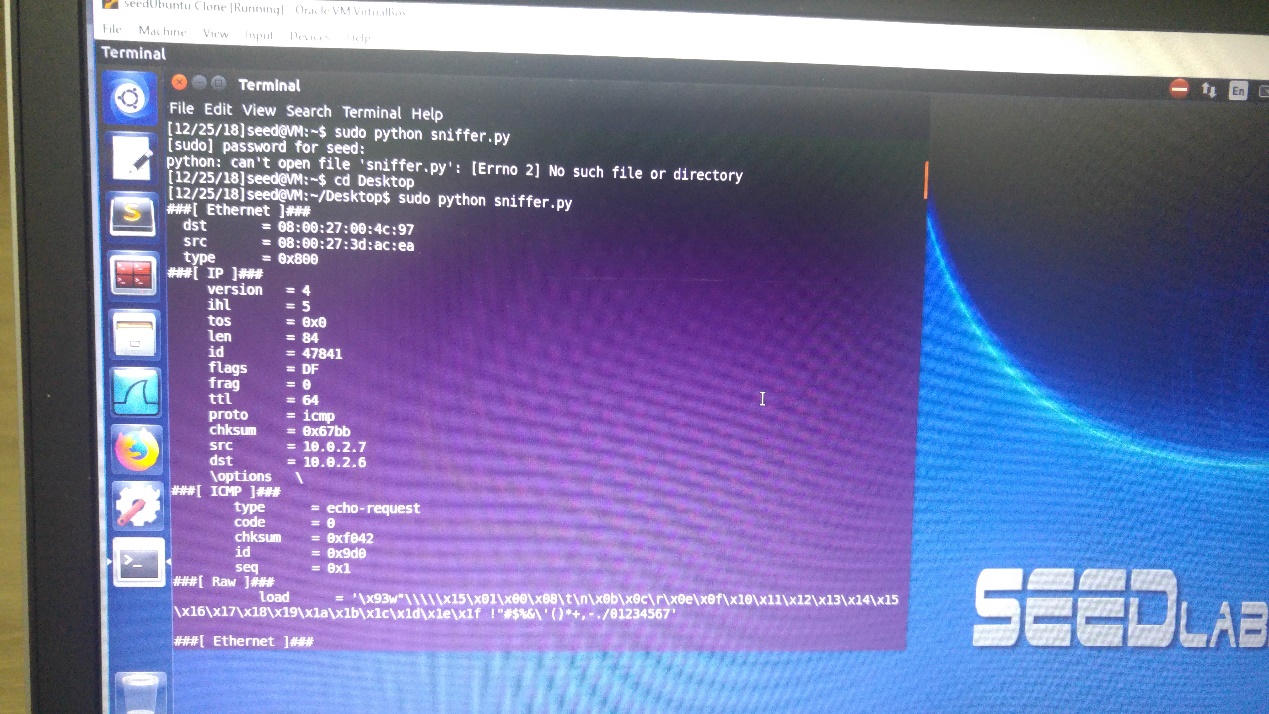
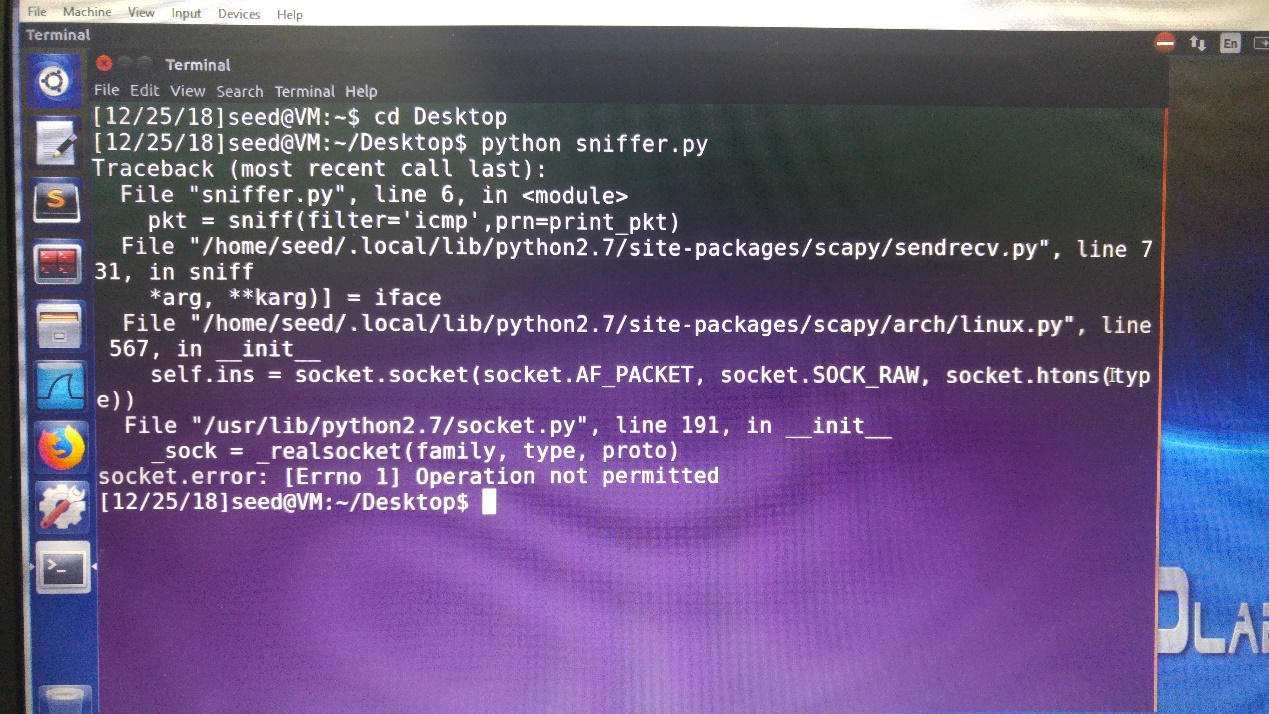
מטלה 6 :

**שאלה 1.1A –**

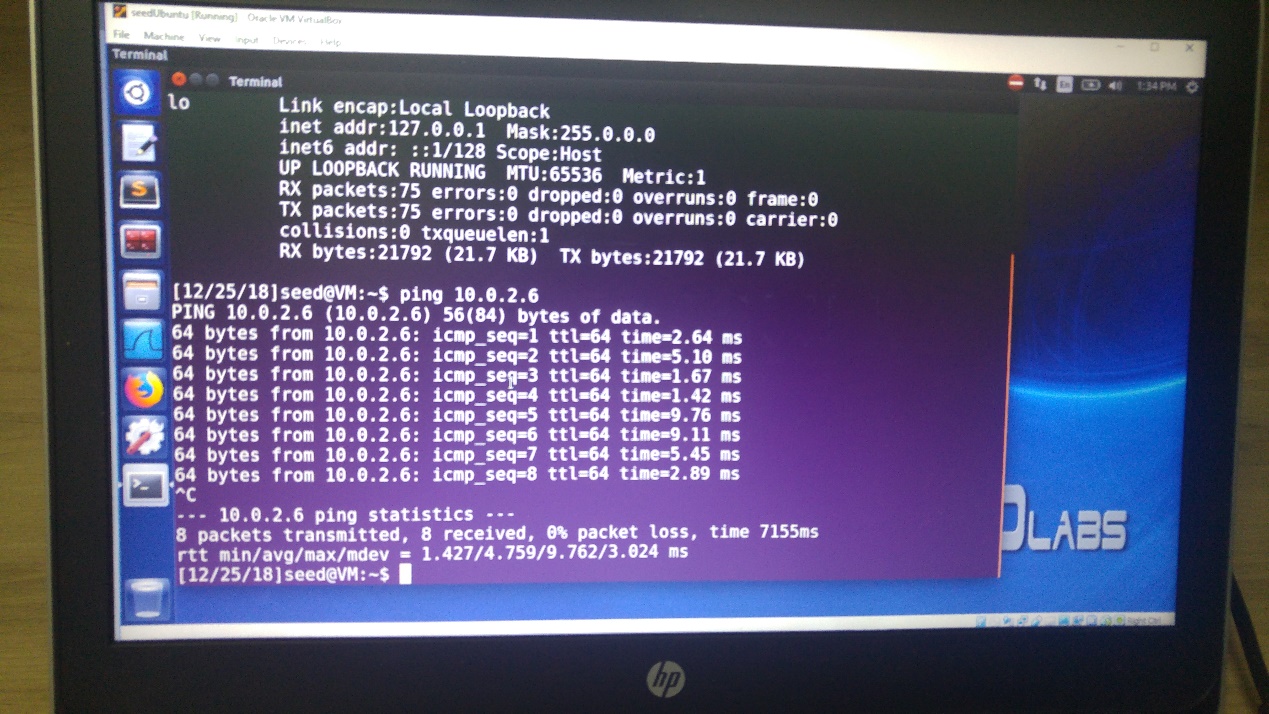
הפעלת הSniffer וגם תפיסת פקטה עם גישת Sudo



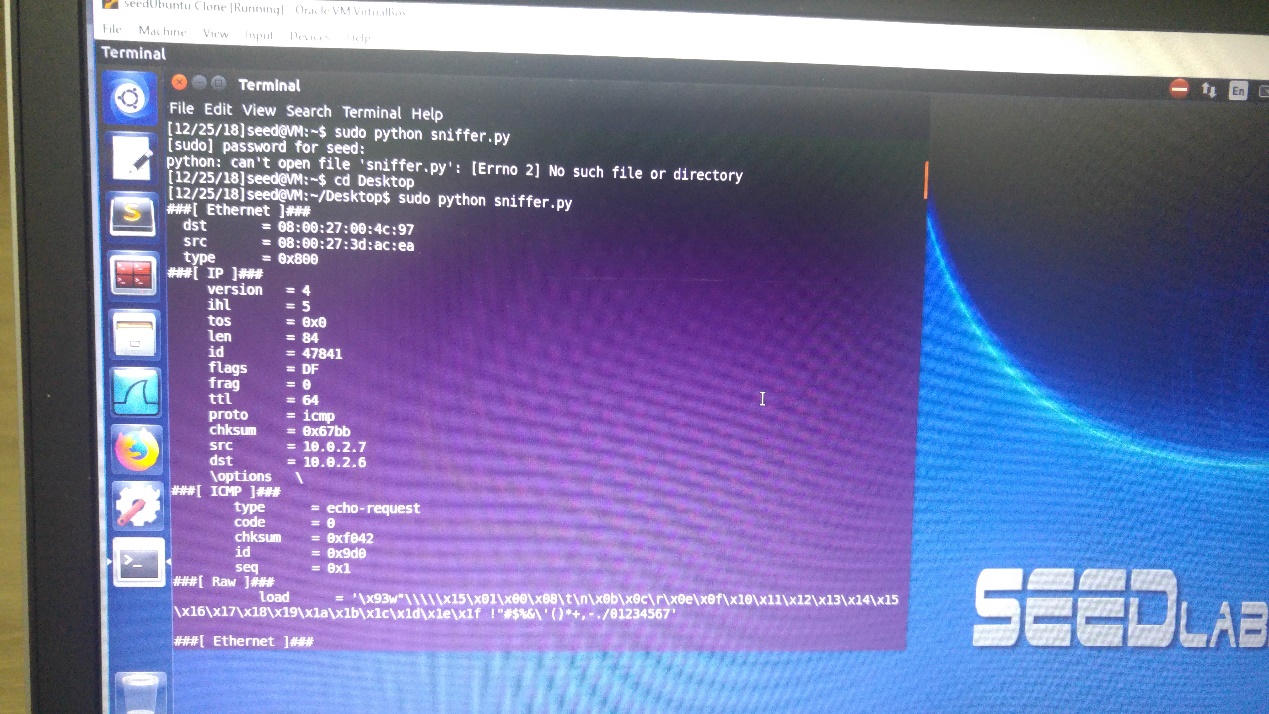
ניסיון להרצת הקובץ ללא גישת שורש ( Sudo)

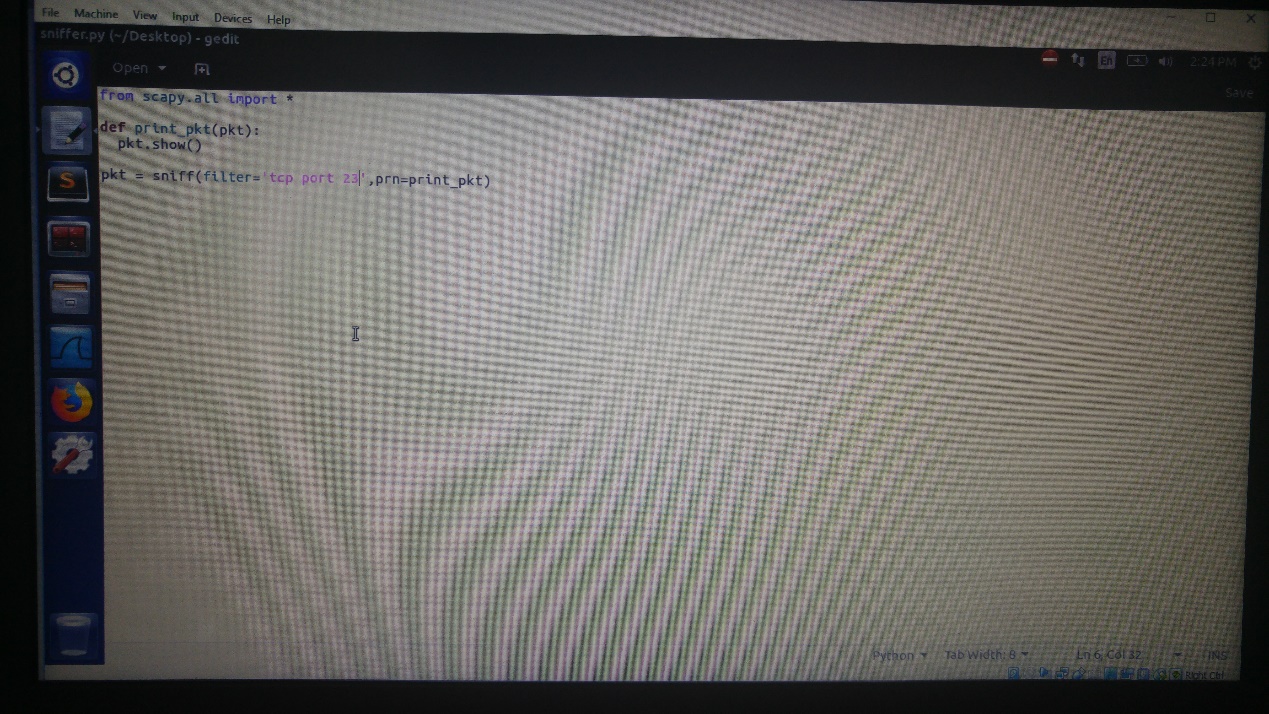
ההבדל בין הרצה עם גישת שורש כלומר מנהל לבין הרצה רגילה הוא שעל ידי גישת מנהל ניתן יהיה לגשת לנתוני הרשת לדוגמא ולנהל אותם דבר שלא היינו מצפים לכל משתמש גישה לכן שמריצים עם גישת שורש של מנהל יהיה ניתן לבצע דברים שקשורים לניהול.

* 1. **B –**

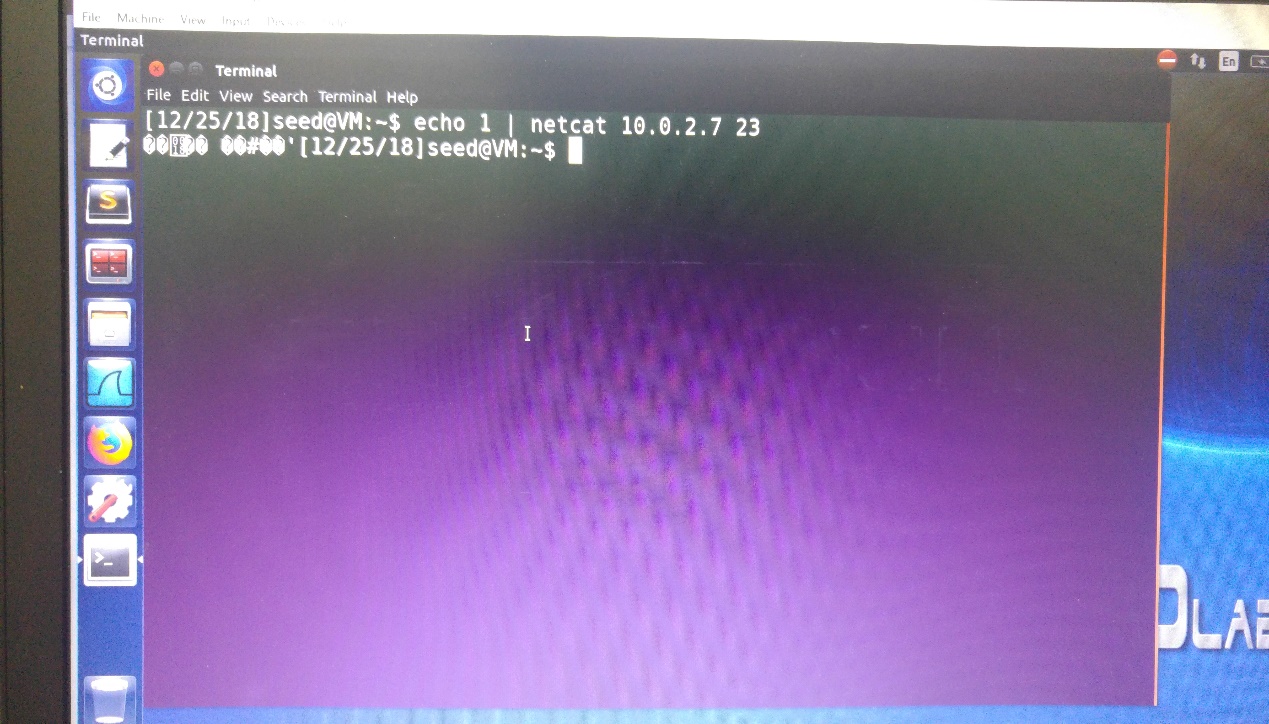
נקודה ראשונה – שליחת ping ממכונה מספר 1 למכונה מספר 2(עם הסניפר)

קבלת הping במכונה מספר 2, נתפס על ידי הסניפר

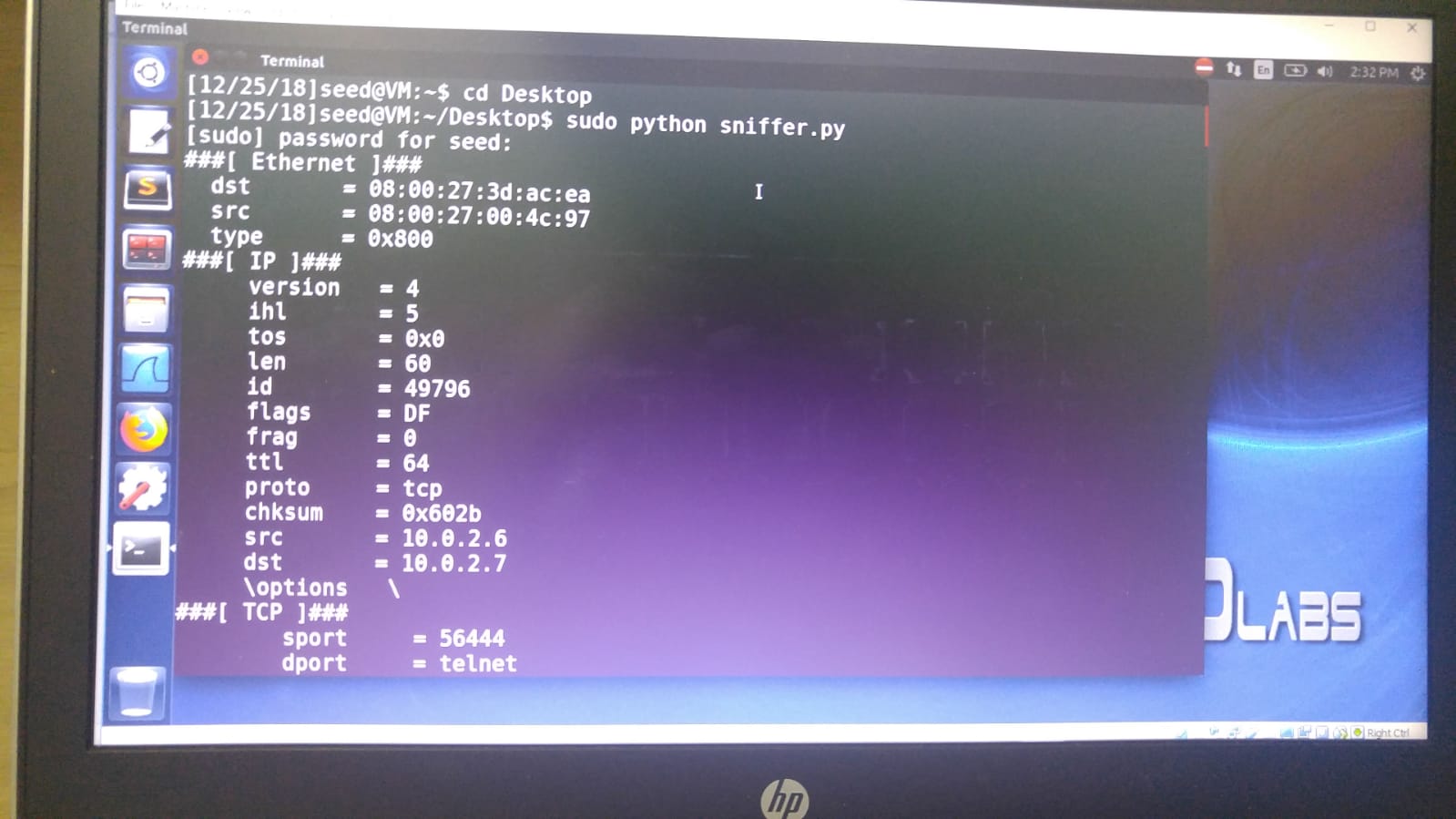


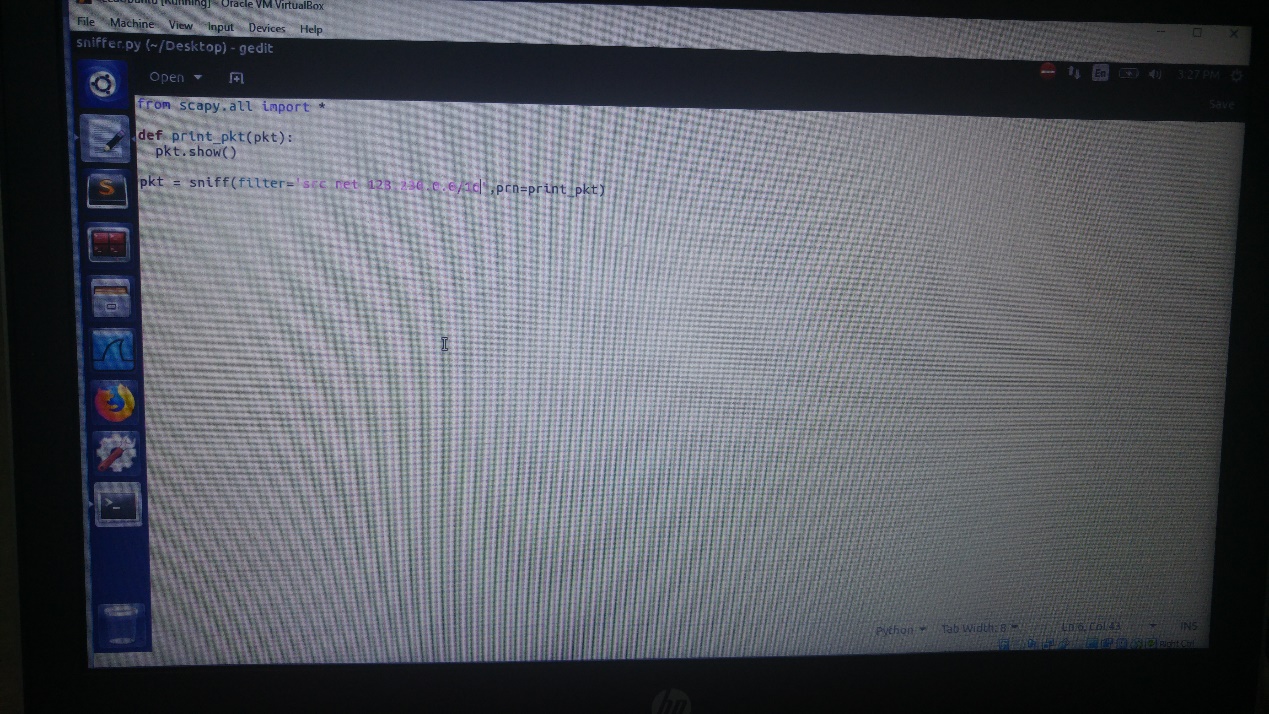
נקודה שניה - code

שליחת הודעת TCP דרך פורט 23 למכונה מספר 2

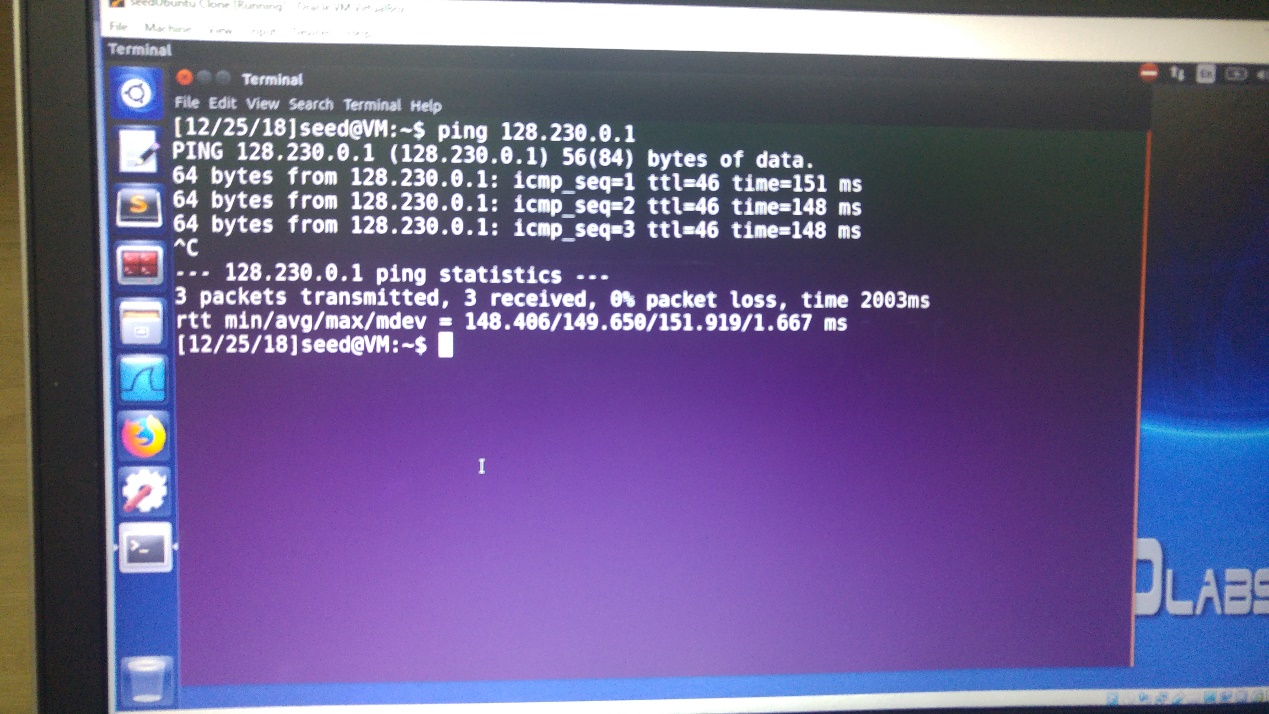


קבלת הפקטה עם הודעת הTCP במכונה מספר 2

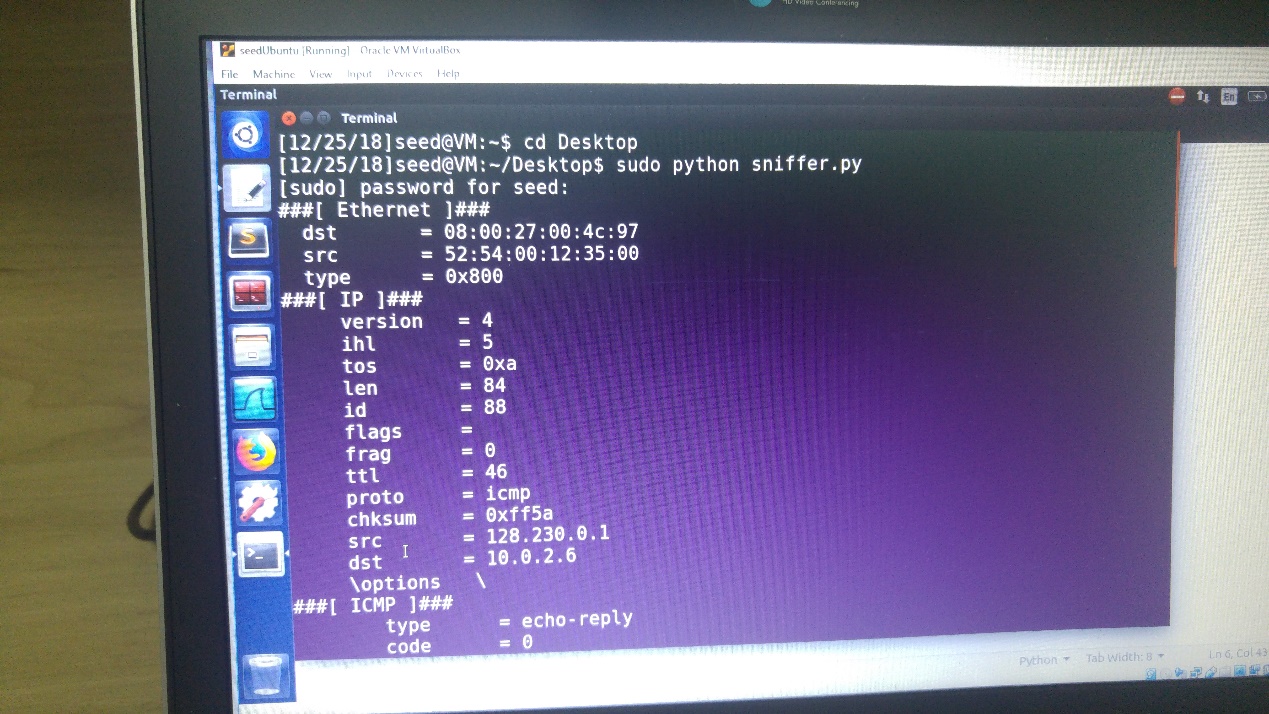


נקודה שלישית - code

שליחת הודעת ICMP למכונה שנמצאת subnet

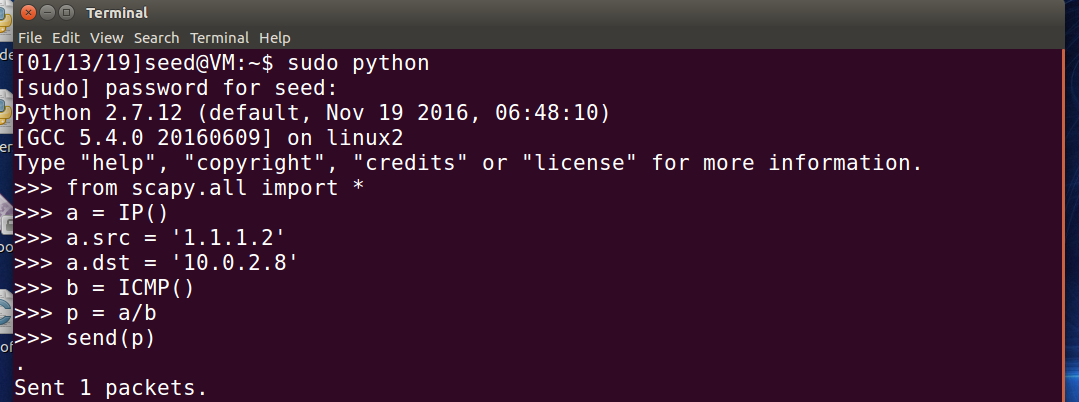


קבלת הפקטה במכונה עם הסניפר

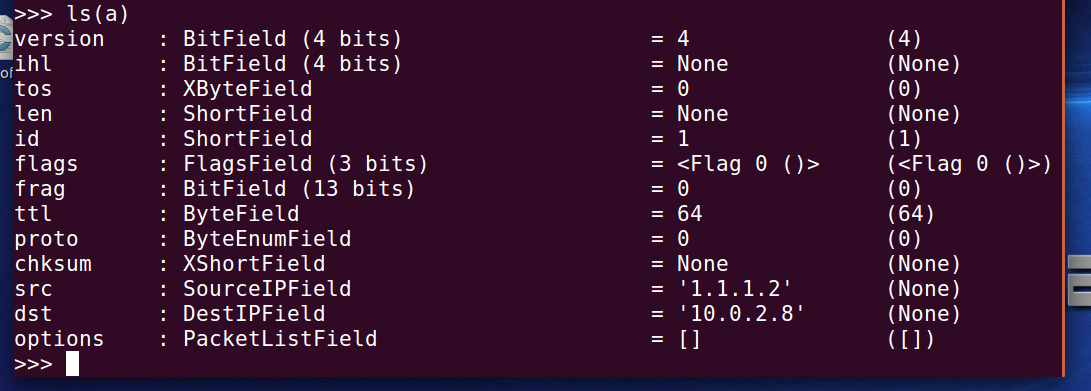


**שאלה 1.2 –**

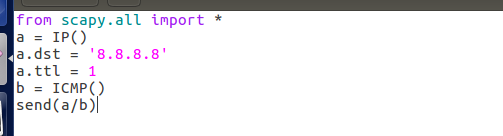
שליחת פקטה לכתובת שרירותית

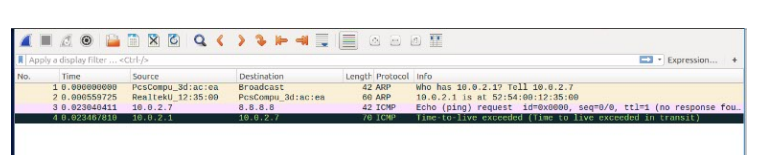


ניתן לראות איך הפקטה נראית

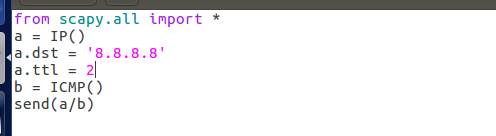


**שאלה 1.3 –**

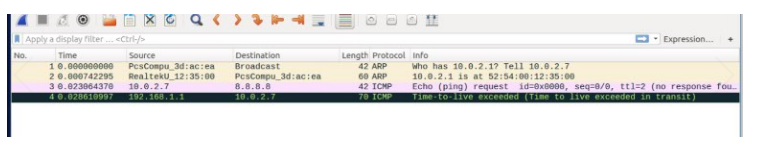
קוד ש ttl = 1 

התוצאה 

ניתן לראות שאחרי "זמן חיים" של הפקטה הוא 1 אז היא לא מגיעה ליעד שלה

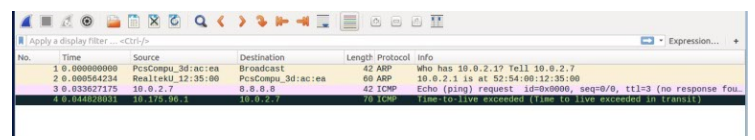
קוד ש ttl = 2 

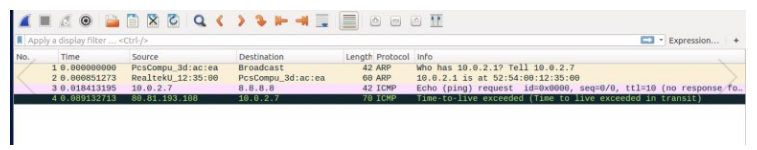
התוצאה



ניתן לראות שגם כאשר ttl = 2 הפקטה לא מגיעה ליעד

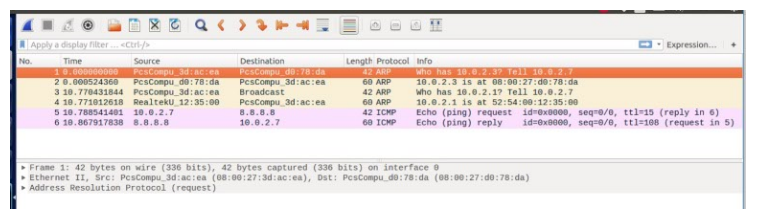
. . . .

ttl = 3 

ttl = 10 

ניתן לראות שעד זמן חיים 10 הפקטה לא מגיעה ליעד

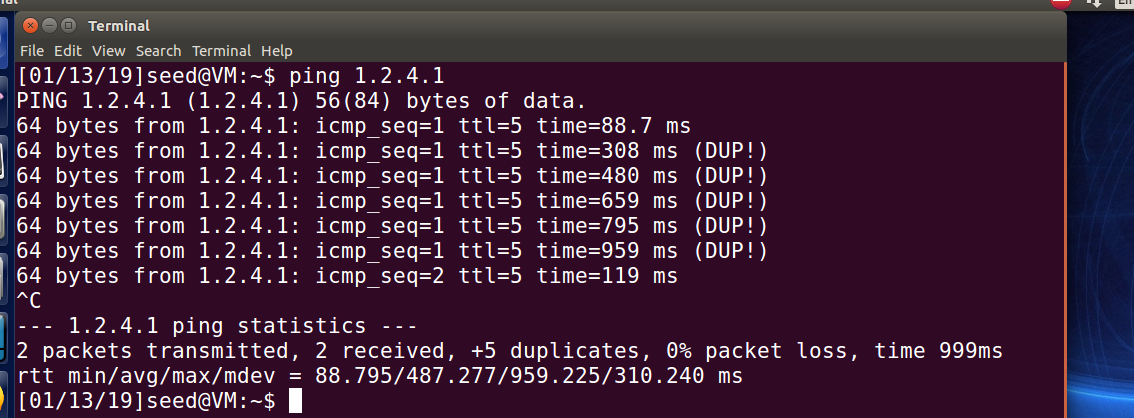
. . . .

ttl = 15 

ניתן לראות שאם ttl = 15 אז הפקטה מגיעה ליעד .

**שאלה 1.4 –** מכונה מספר 1 שולחת ping לכתובת שרירותית ומכונה מספר 2 מסניפה את הודעת ICMP ובונה הודעה מזוייפת שאותה היא מחזירה בחזרה למכונה מספר 1 כביכול מהיעד שמכונה 1 ציפתה לקבל ממנו מענה:

מכונה מספר 1 שולחת ping

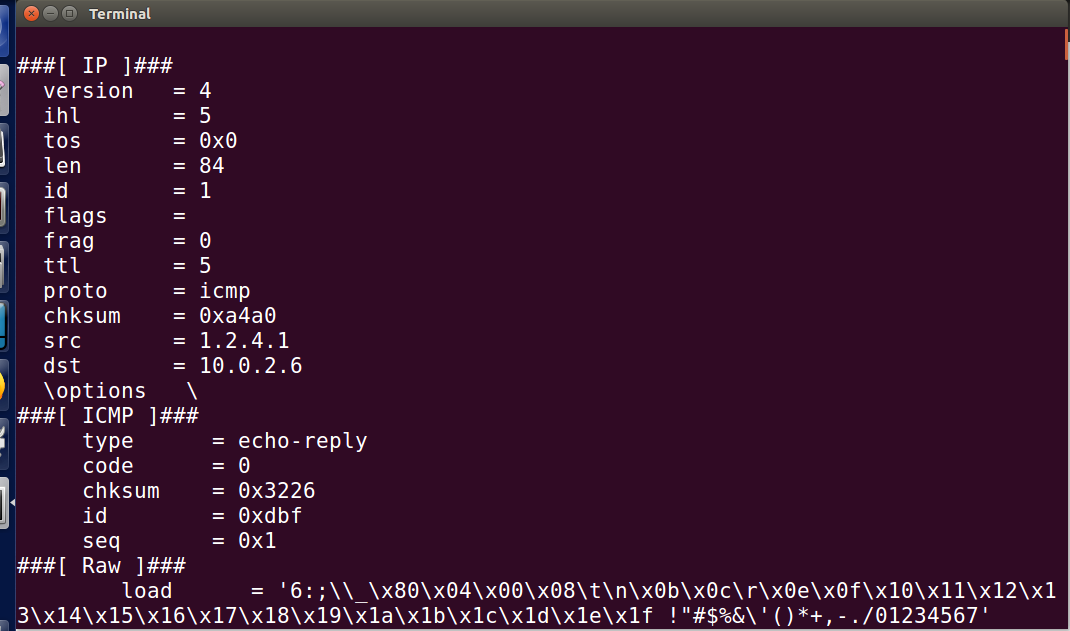


מכונה מספר 2 מסניפה פקטות ICMP



מכונה מספר 1 שלחה פקטה לכתובת מסוימת

ומחזירה פקטה מזוייפת למכונה מספר 1



מכונה מספר 2 שולחת פקטה מזויפת

הקוד -

Response

שליחה בחזרה

שם בפקטה החדשה נתונים נוספים כמו אלה

יוצר את הheader של הIP והICMP החדשים והמקור של ההודעה כעת הוא היעד שמכונה 1 שלחה אליו

לוקח נתונים מהפקטה שהסניפר תפס ושומר אותם עבור הפקטה החדשה שניצור