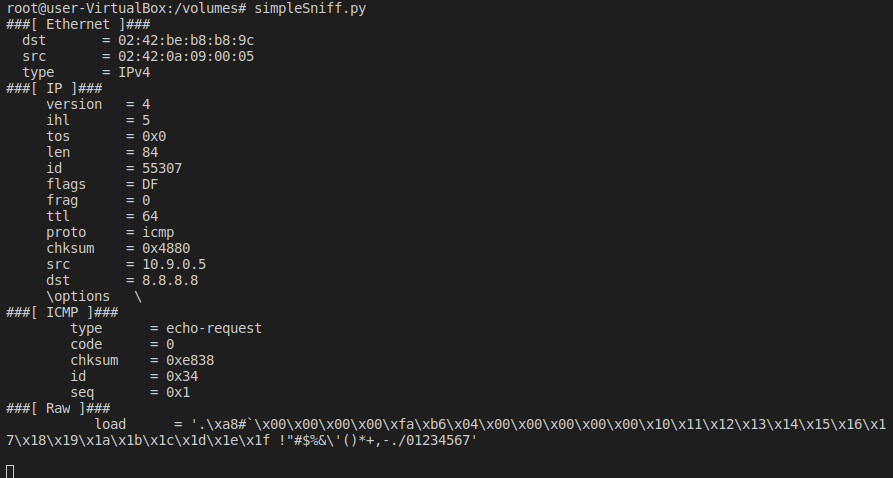
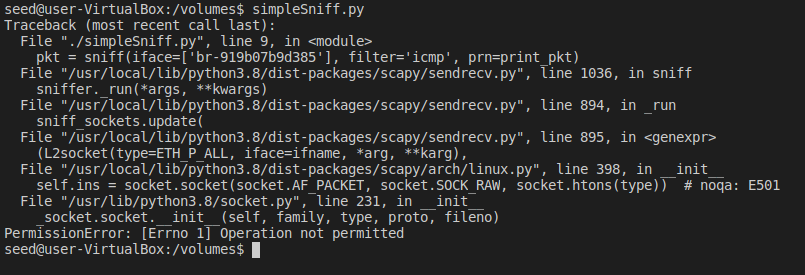
מטלה ברשתות 4

1.1A בהרצה של מנהל הכל עובד





בהרצה ללא גישת מנהל אין לו אישור לרוץ ולכן נותן שגיאת not permitted כי אין אישור לקוד לגשת לכרטיס הרשת הווירטואלי



1.1B

ICMP

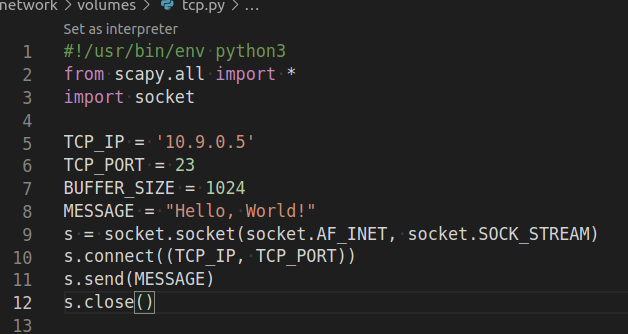


ומצורפת תמונה של הרצה בתת שאלה קודמת

TCP with ip:10.9.0.6 dest port:23

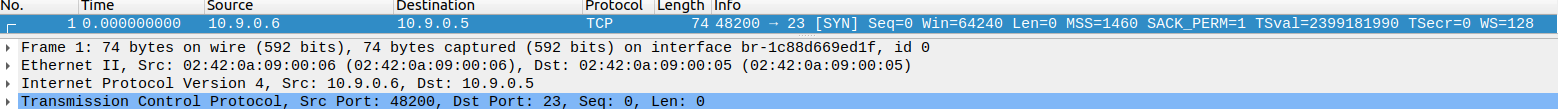
הוספנו עוד משתמש ל-containers ומשם שלחנו לאחד המשתמשים האחרים הודעת TCP בזמן שהקשבנו עם ה-attacker

דוגמת הקוד שנשלחה:

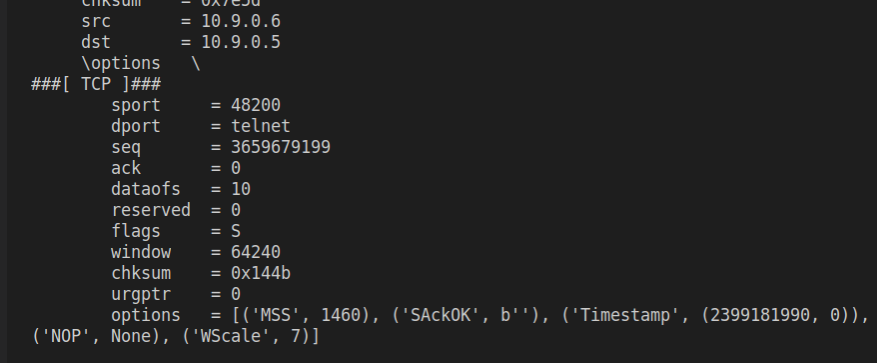


התוצאה:

ב-wireshark



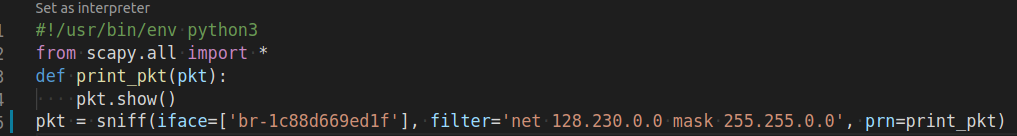
ב-attacker



Subnet:

שלחנו ping לכתובת 128.230.61.171 מכתובת 10.9.0.6

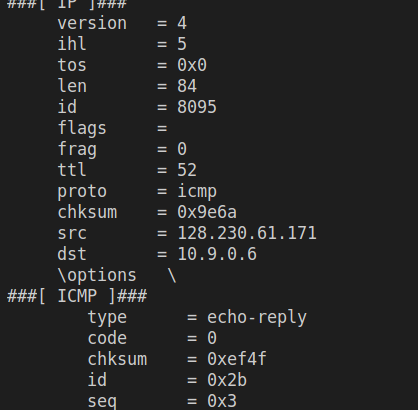
דוגמת הקוד שבצענו sniffing



התוצאה ב-wireshark



ב-attacker

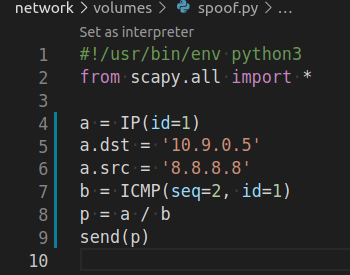


**Task 1.2**

ביצענו spoofing כך:

יצרנו פקטה b שהיא פקטת ICMP ויצרנו פקטה a שהיא פקטת IP ושינינו את הsrc שלו להיות "8.8.8.8" (גוגל) ואת ה-dest שלו להיות אחד מה-host שלנו בכתובת "10.9.0.5" ואז שלחנו אותה אל ה-host והוא הגיב בecho reply לכתובת "8.8.8.8".

הקוד:



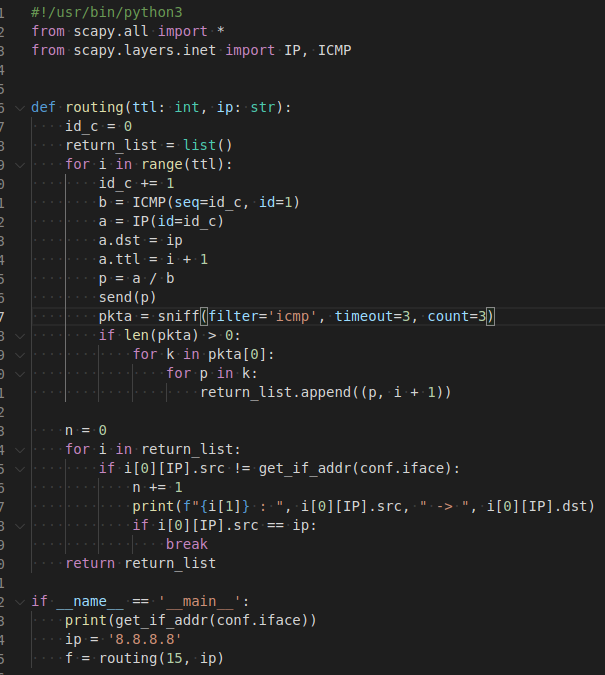
התוצאה ב-wireshark

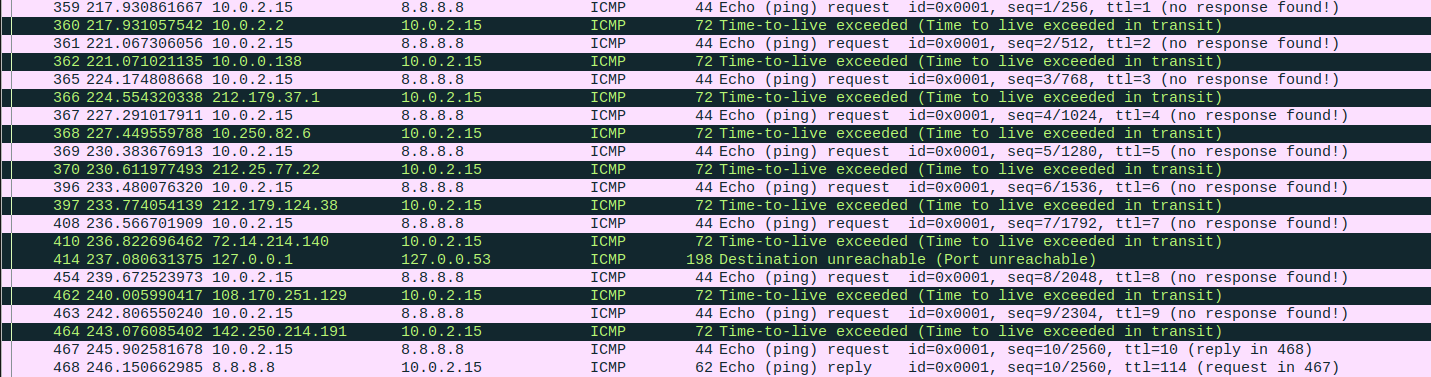


**Task 1.3**

כתבנו את הקוד של ה-traceroute שבעצם שולח 15 פקטות של icmp כל אחת עם TTL אחד יותר מהשני וניסינו גם לבצעsniffing בקוד עצמו והוא עובד אבל לא מושלם ולכן נסתפק בתמונה מה-wireshark כדי להראות שאכן גילינו את כל הראוטרים שבדרך.

הקוד:

****

התוצאה ב-wireshark

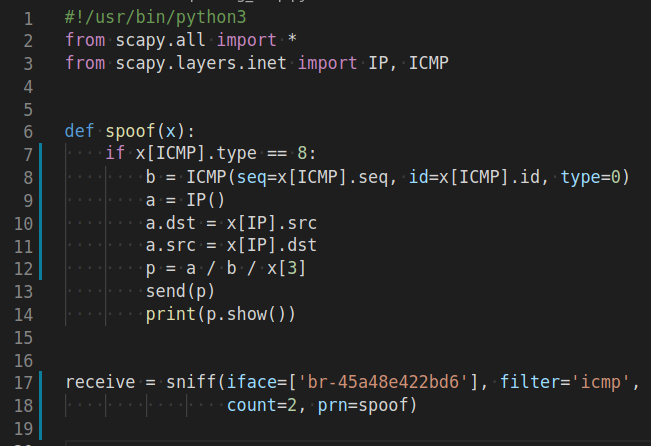
ניתן לראות בעמודה זו את כל הראוטרים שבדרך עד שמגיע אל היעד שלו שהוא 8.8.8.8

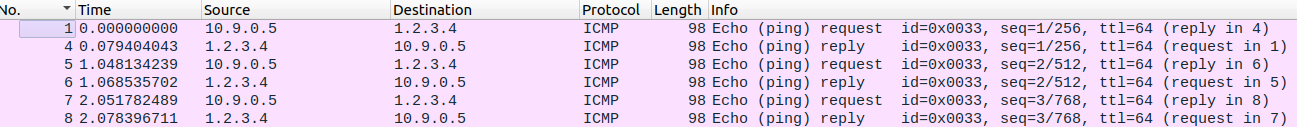
**Task 1.4**

שלחנו הודעת ICMP לכתובת 1.2.3.4 שלא קיימת מתוך ה-host שלנו, ולא קיבלנו תגובה חזרה,

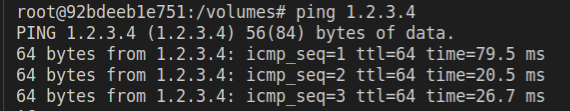
בתוך ה-Wireshark :

ואז הפעלנו את הקוד spoofing שלנו כאן:

ושלחנו שוב הודעת ICMP בעזרת ה-ping המובנה בלינוקס, והפעם קיבלנו הודעת reply שזייפנו.

תמונת -Wireshark

תמונת הקבלה מהטרמינל:



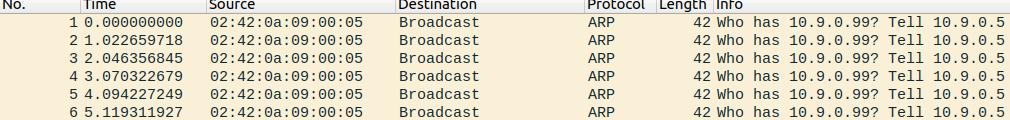
**לכתובת 10.9.0.99**

שלחנו הודעת פינג אך קיבלנו רק תשובה ש-

Destination Host Unreachable

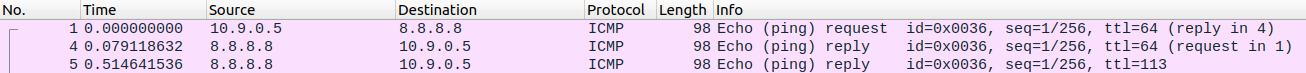
ובמבט על ה-wireshark נראה כי ה-host שולח הודעת broadcast ARP ומחפש למי יש את הכתובת הנ"ל אך ללא תשובה, וכיוון שכתובת זו צריכה להיות קיימת בתוך הרשת הפנימית בגלל ה-subnet mask שלה, היא אמורה להחזיר תשובה אך היא באמת אינה קיימת ברשת הפנימית, ולכן אינו שולח בכלל הודעת ICMP ולכן לא ניתן לבצע spoofing. (אם רוצים בכל זאת לבצע spoofing צריך לבצע זאת ע"י הקשבה להודעת ה-ARP)

התוצאה ב-wireshark:



**לכתובת 8.8.8.8**

שלחנו הודעת ping וקיבלנו הודעות reply חוזרות, ומידי פעם הודעות reply משוכפלות ,מכיוון שגם מערכת ה-spoofing שלנו החזירה תשובה וגם הכתובת 8.8.8.8 החזירה תשובה.

התוצאה ב-wireshark: