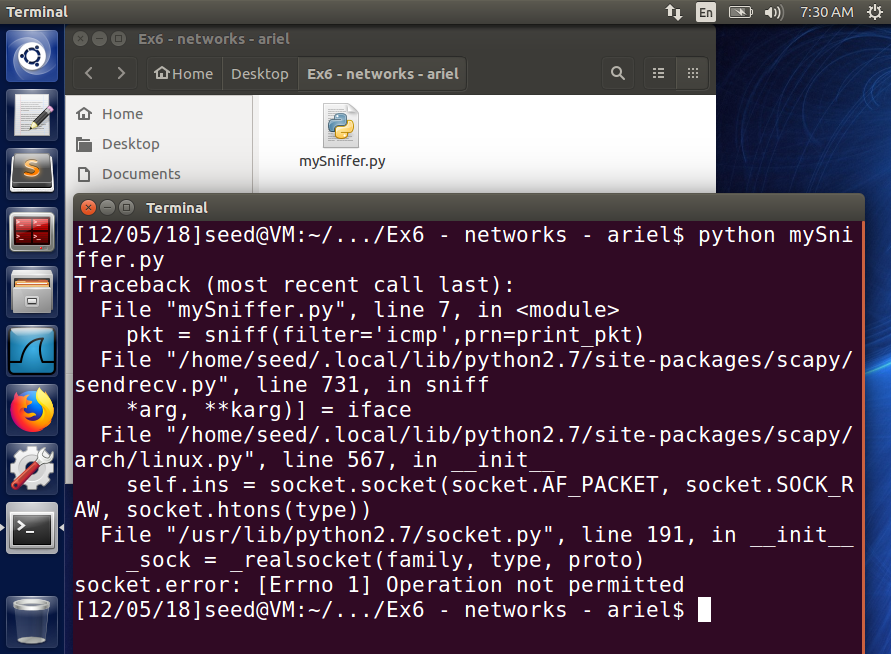
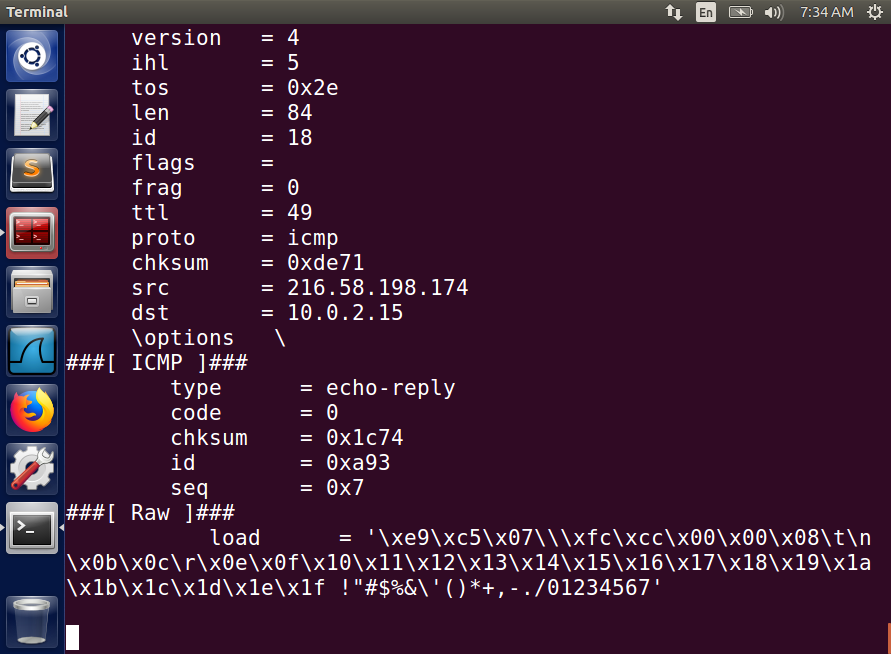
**עבודת הגשה 6 – Sniffing Spoofing**

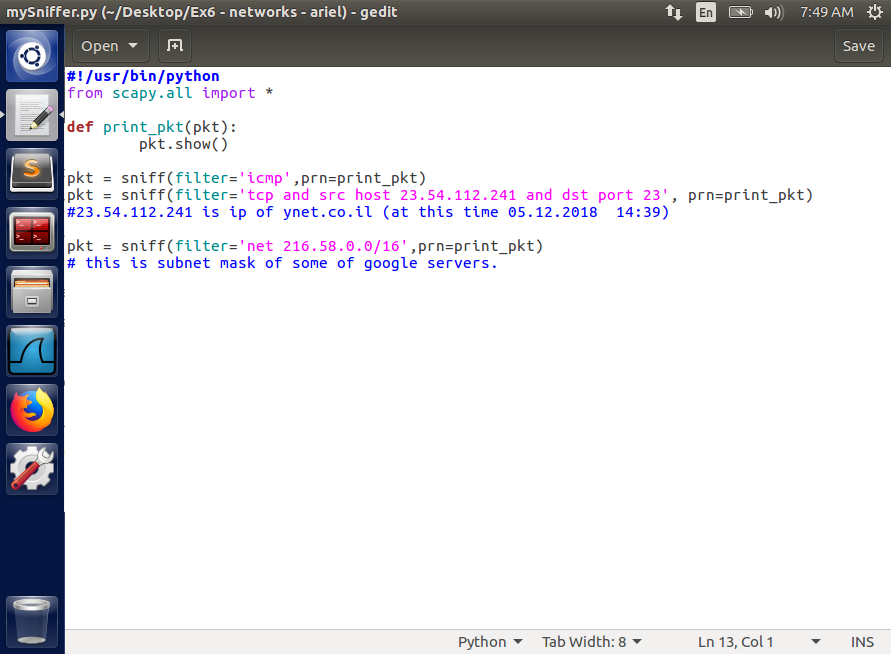
**מגישים:**ליעד כהן 316602630

תימור שרעבי 311508220

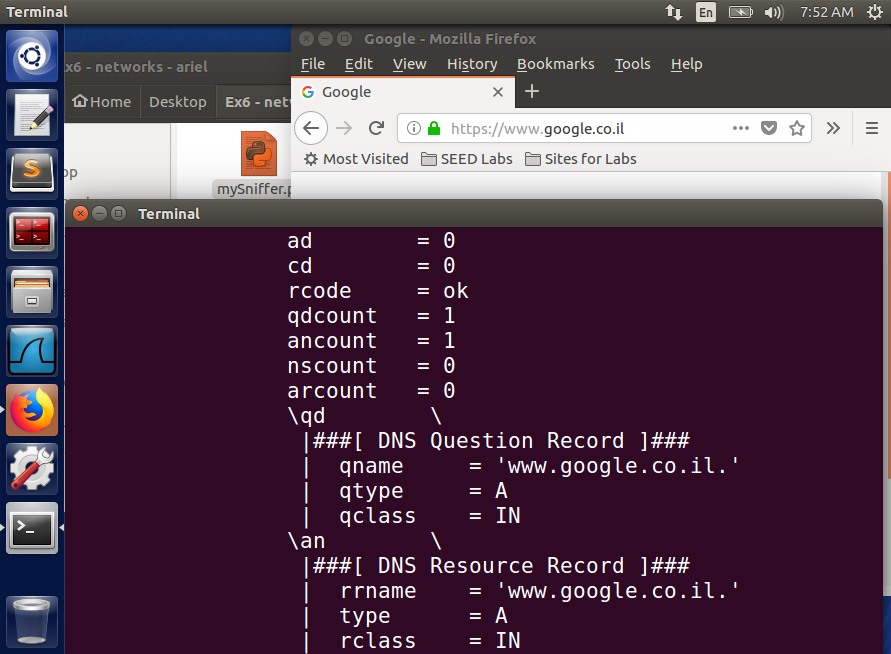
1. התקנו את ה SEEDvm והפעלנו ב virtual box .
   1. **א': Task 1.1A** ריצת קוד הסנפה ללא הרשאות אדמין:   
      קיבלנו תשובה operation not permitted.  
      



ריצת קוד הסנפה עם הרשאות אדמין: הצלחנו לתפוס פאקטה !

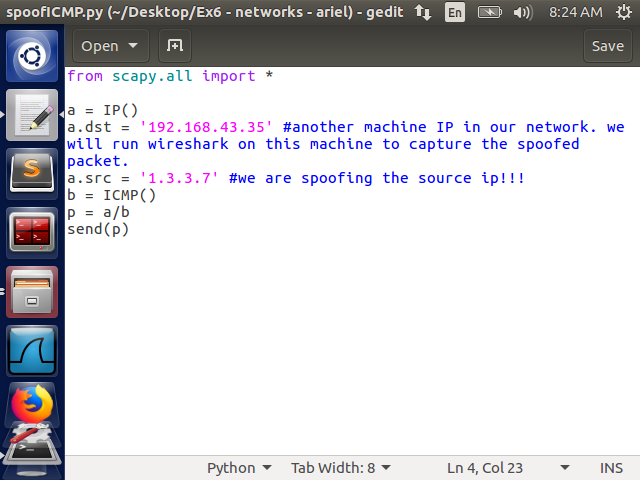
**1.1 ב': Task 1.1B** שינוי קובץ ההספנה שלנו שיכיל את הפילטרים הנוספים (כל אחד בנפרד כפי שנתבקשנו, אבל שבאותה תכנית).

ריצה של ההסנפה עם הפילטרים הרלוונטים, כניסה לאתר google.com (שהוא חלק מהסאבנט בפילטר השני שרשמנו) ותפיסת הפאקטה.

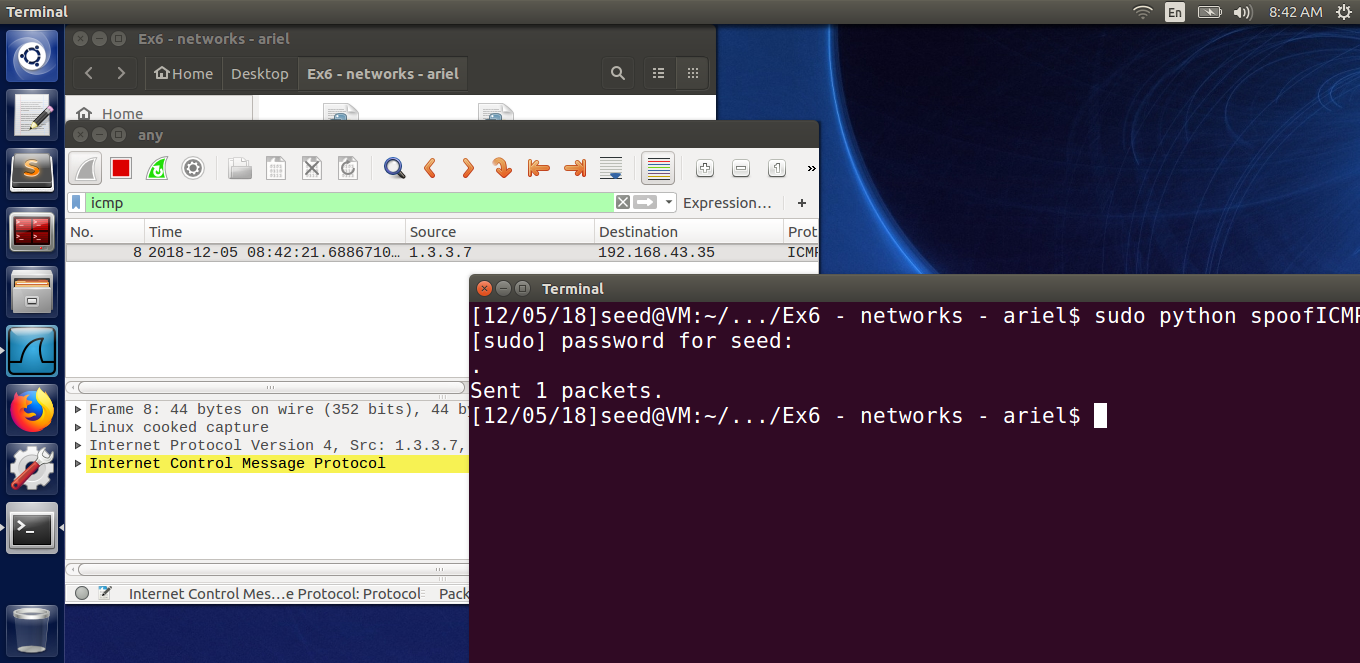


**Task 1.2: Spoofing ICMP Packets**

נשנה את הsrc ip שלנו לאייפי שונה כלשהו, נשנה את ה dst ip לכתובת IP של מחשב ברשת שלנו, ובאותו מחשב ששלחנו נפתח WIRESHARK לראות את הפאקטה שנשלחה שם – ונבדוק מה ה SOURCE שלה!



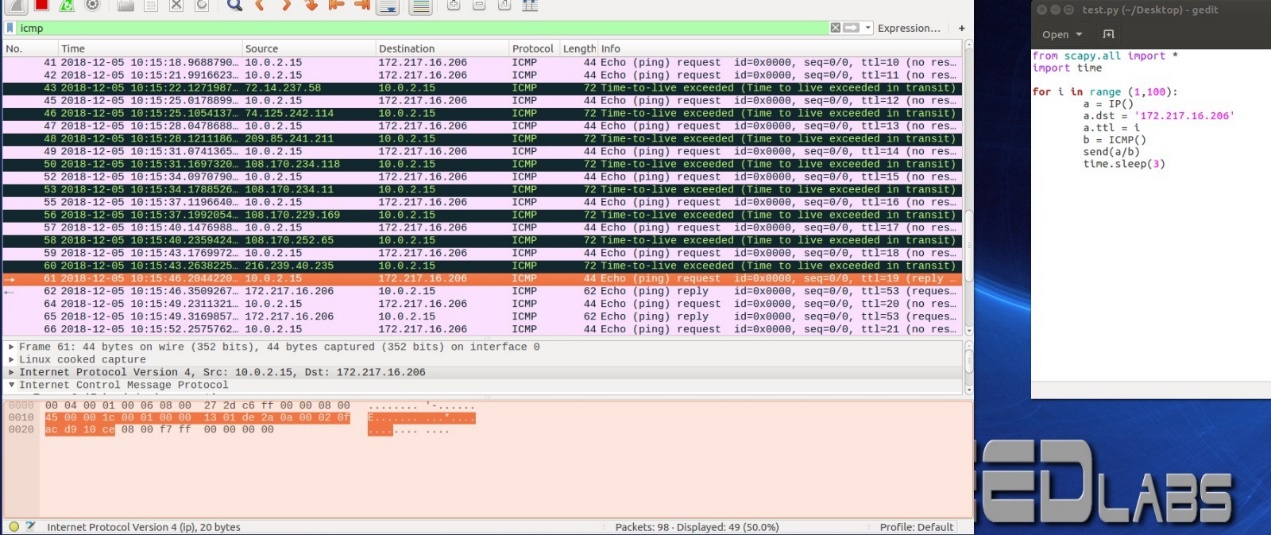
ואכן הSOURCE של הפאקטה הוא 1.3.3.7 כפי שרשמנו.



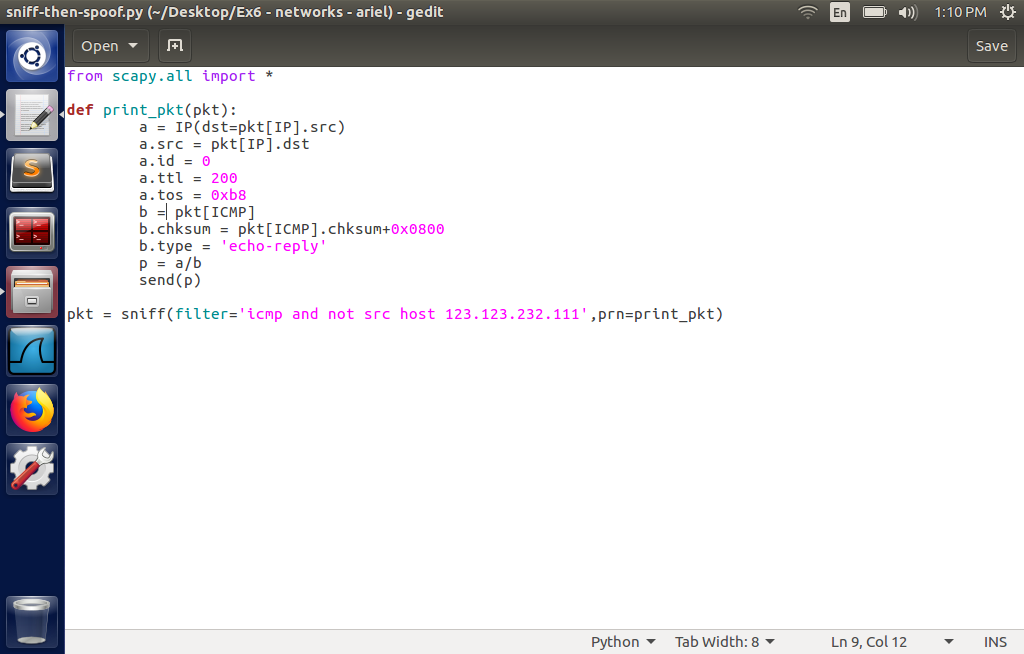
**Task 1.3: Traceroute**

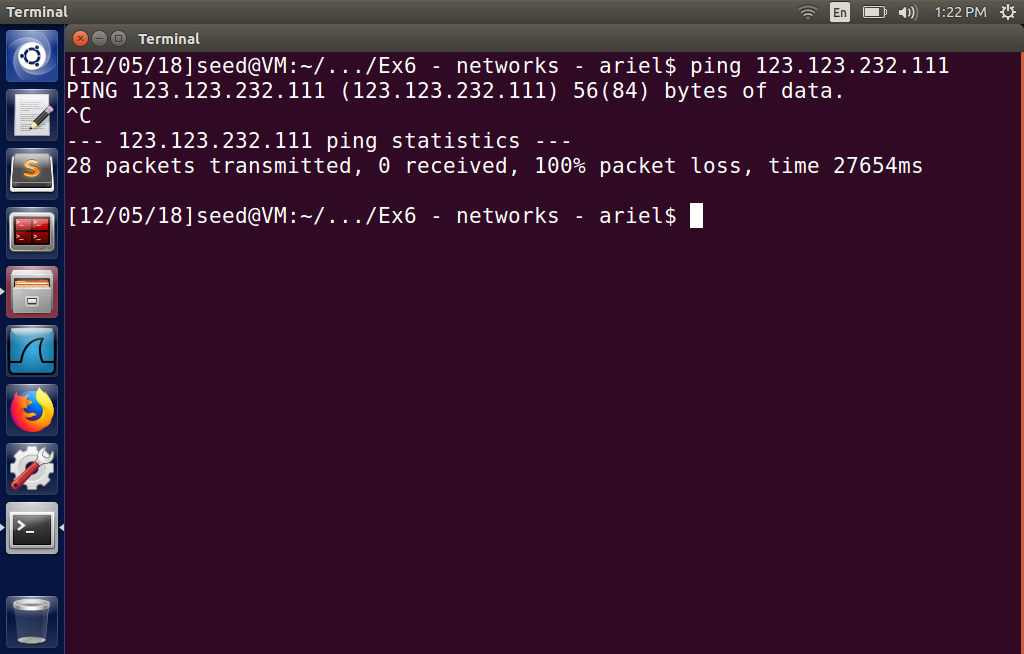
נבדוק כמה ראוטרים 'עומדים' בין ה VM שלנו לבין google.com (216.58.213.110).

רשמנו קוד שירוץ אוטומטי בפייטון.

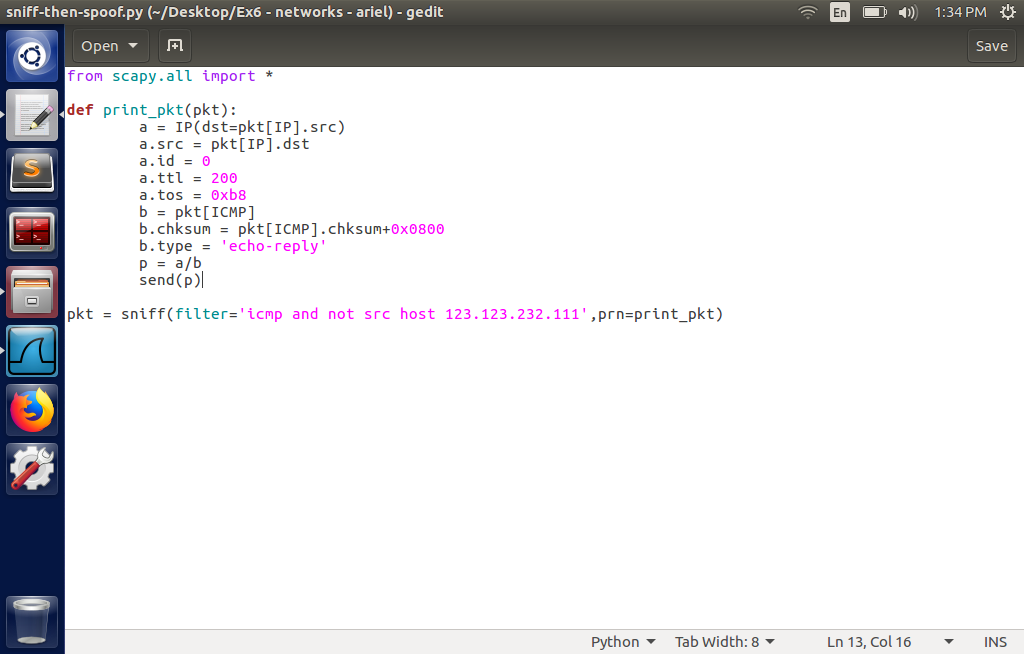
בTTL 19 כבר קיבלנו תשובה. לכן 19 ראוטרים.

**Task 1.4: Sniffing and-then Spoofing**

מצאנו אייפי שלא מגיע לשום מקום: 123.123.232.111. הנה : (קוד בעמוד הבא!)



בנינו קוד למכונה 2 שתתפוס פאקטות שנשלחות כ ICMP .   
ברגע שהתקבלה פאקטה , אנחנו נקרא לפונקציה חדשה שבנינו שהיא תבנה פאקטה חדשה- היעד שלה הוא הכתובת מקור של הפאקטה שתפסנו (המקורית),   
הכתובת מקור היא כתובת היעד (שלא באמת קיים).   
אנחנו מעדכים את ה Checksum והID וה type כדי שהפאקטה תתקבל כ reply לבקשה המקורית. זה הקוד שלנו:



כעת הרצנו את ה sniffer-then-spoof.py במכונה 2 ובמכונה 1 עשינו פינג לכתובת שאין בה אף אחד. 123.123.232.111. אנחנו אמורים לקבל תשובה שהיעד לא נמצא, אבל מכונה 2 עושה SPOOF ומחזירה פאקטה למכונה 1, ככה שמכונה 1 רואה כאילו היעד קיים!!!

