מטלה 6 – 213101637

בסוף השאלות מצורפים הסברים וצילומים של הפלט

שאלות מהמטלה –

1.1.A

בתור ה"מחשב" שיצר הדוקר לא היה צריך להשתמש בסודו כדי להריץ את הקבצים, זה כנראה בגלל שהם קיבלו הרשאת ROOT מהתחלה (ניתן לראות זאת על ידי יצירת קובץ או תקייה דרכם ואז רואים שהתקייה נעולה ולא ניתן למחוק אותה בליה הרשאת ROOT מה שקורה כשיוצרים תקייה כשאתה עם הרשאת ROOT)

2.1.A

הפונקציה הראשונה (PCAP\_OPEN\_LIVE) אומרת להתחיל להסניף על האינטרפייס שנותנים לה

הפונקציה השנייה(PCAP\_COMPILE) מקמפלת את הפילטר שנתנו לה לפי הBPF שזה ההוראות איך לקמפל בעצם

הפונקצייה השלישית(SET\_FILTER) מציבה את הפילטר

הפונקצייה הרביעית(PCAP\_LOOP) היא לולאת ההסנפה, היא אומרת לאיזה פונקציה תלך כל פקטה שהסנפנו ושומרת אותה בבאפר

אנחנו צריכים הרשאת ROOT כי אנחנו ניגשים לכרטיס הרשת או יכול להיות שהספרייה משתמשת גם בRAW\_SOCKET שגם דורש הרשאות ROOT

ההבדל הוא היכולת להסניף פקטות העוברות ברשת הפנימית, ללא מצב זה נוכל להסניף פקטות הבאות אלינו או יוצאות ממנו וכאלה עם IP לוקלי כלאמר 127.0.0.1 או 0.0.0.0

2.1.c

את הסיסמא ניתן לראות דרך הפלט לאחר שמודפס PASSWORD תיהיה הסיסמא אות אות כאשר כל שורה האות האחרונה שלה האי חלק מהסיסמא

2.2.B

כן, לגודל המקסימלי של פקטה, מכיוון שאם יהיה גדול מזה לא נוכל לשלוח את כל הפקטה בכלל אבל אם הכוונה שבכללי לא משנה אם ישלח כל הפקטה או לא אז התשובה היא לא כי הגודל שלו משתנה בהתאם לקלט

כן, כי אתה בונה את הפקטה ולכן המחשב לא יעשה זאת בשבלך

אנחנו צריכים להיות ROOT בגלל שככה המחשב מבקש כשתמשים בRAW SOCKET וזה כדיי למנוע גישה בעצם לדברים שיכולים לפגוע בפעילות המערכת

הקוד יקרוס פה sock = socket (AF\_INET, SOCK\_RAW, IPPROTO\_RAW)

תיעודים-

* 1. ו 1.1A

ההרצה עם הSEED ללא שימוש בSUDO ורואים שאכן הקובץ רץ

A screenshot of a computer

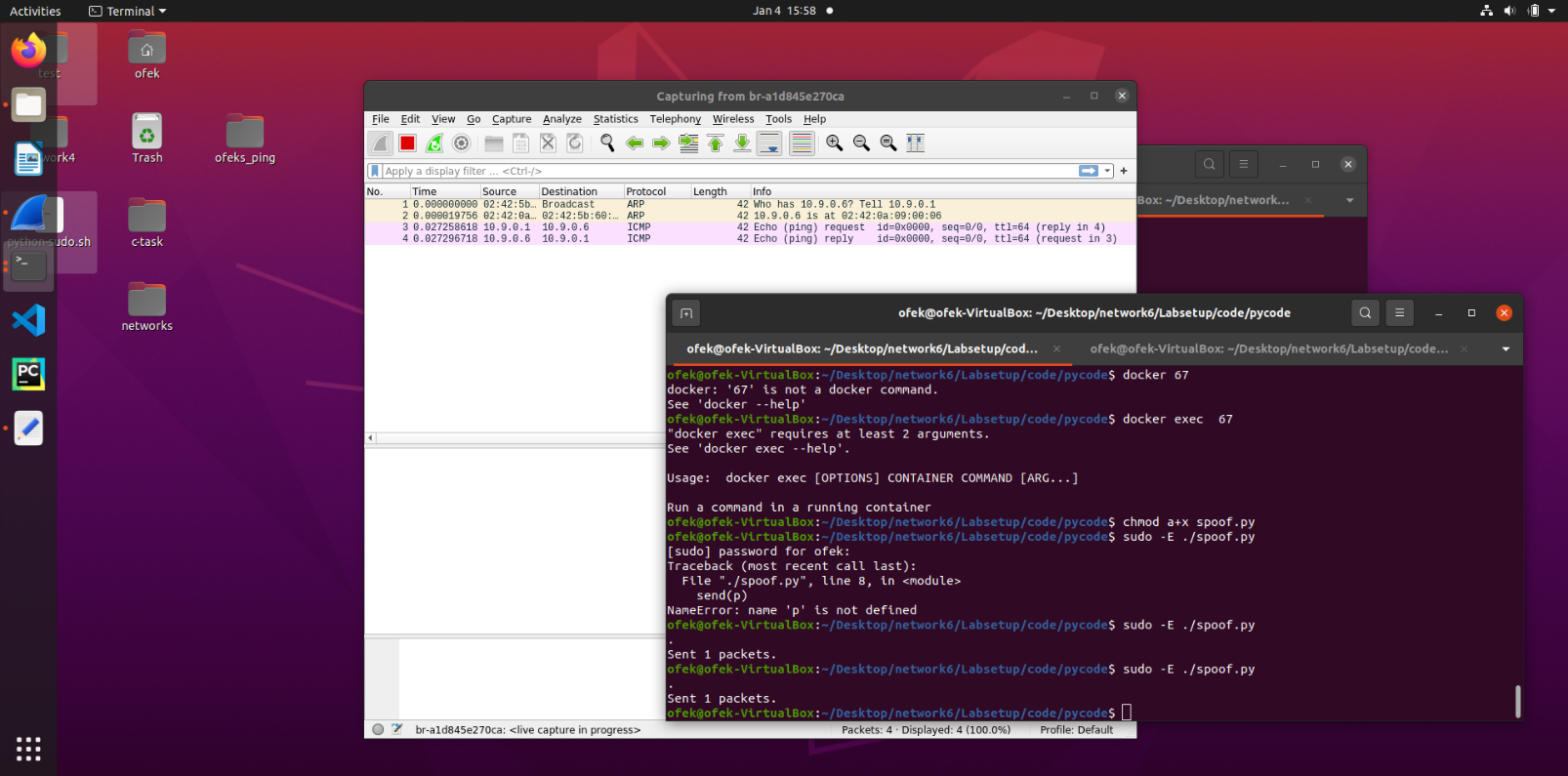
Description automatically generatedוהנה כאשר כן צריך SUDO, ניתן לראות שאכן עובד

A screenshot of a computer

Description automatically generated

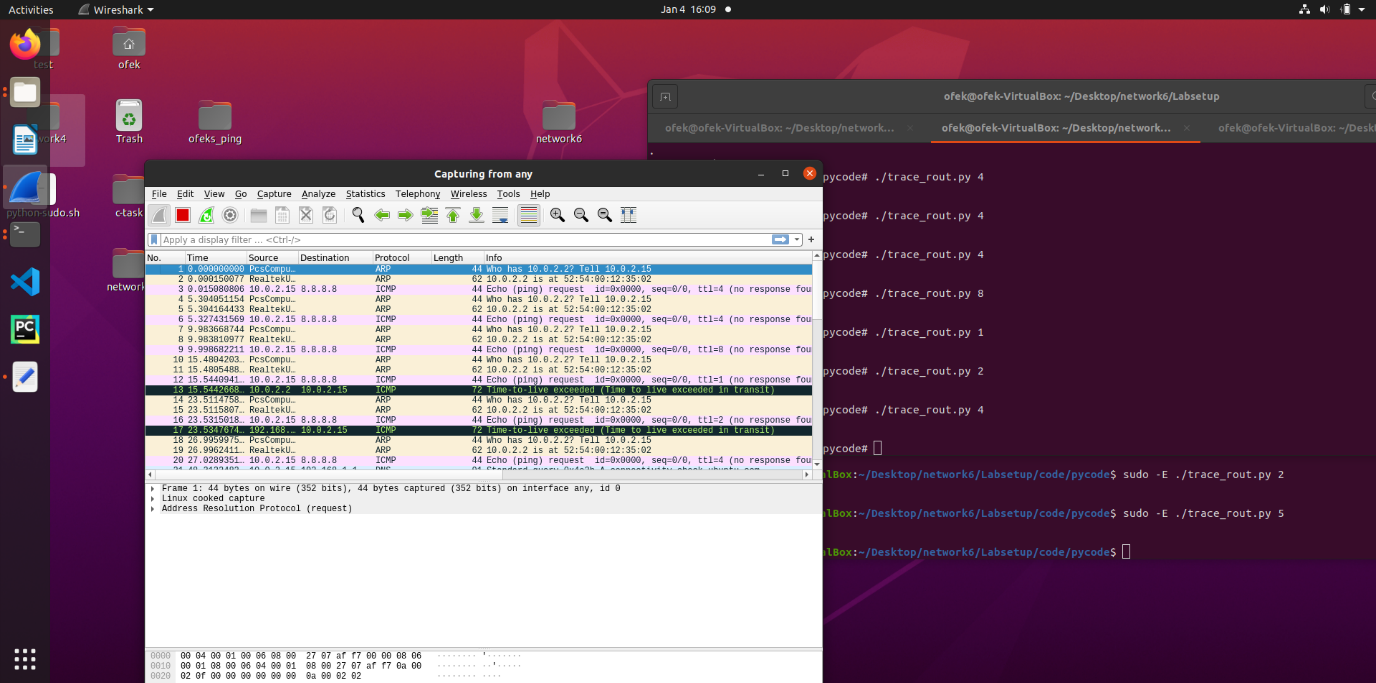
1.2

ספופפינג לכתובת 1.9.0.6, רואים בווירשארק שאכן קיבלנו תשובה וגם ניתן לראות ששלחנו בשורת הפקודה

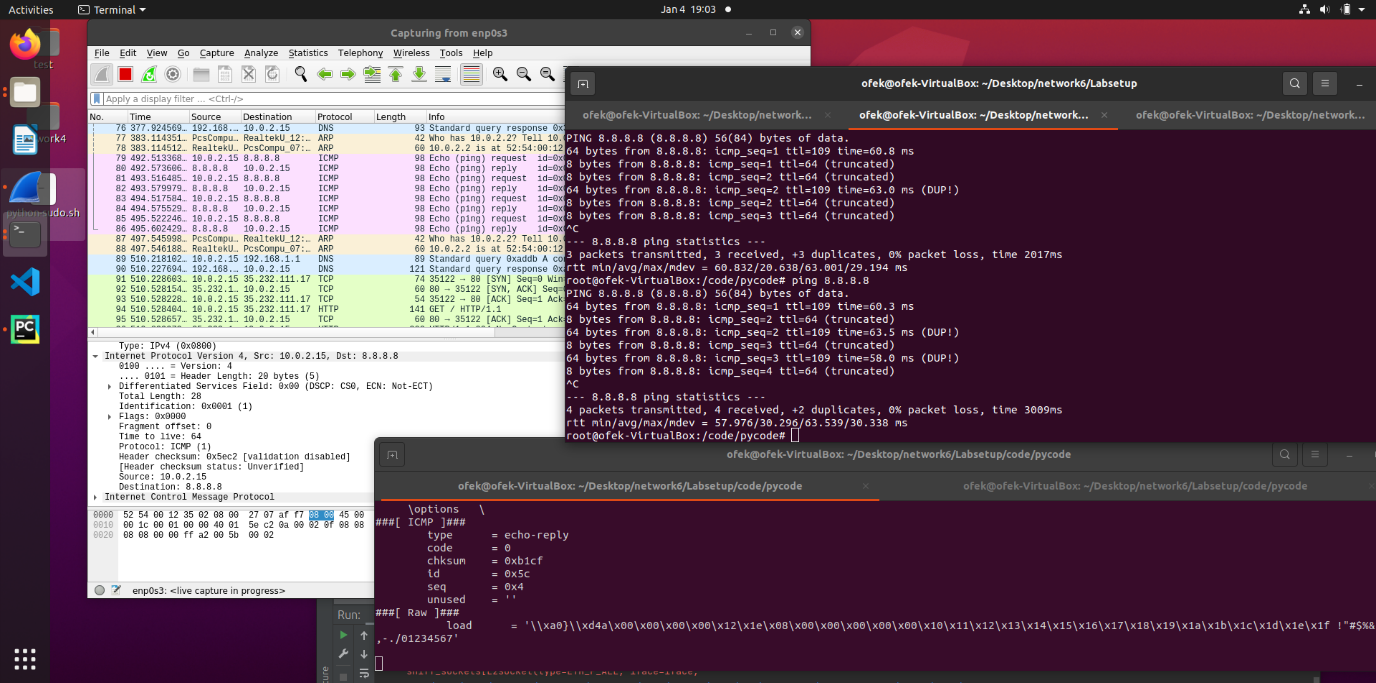


1.3

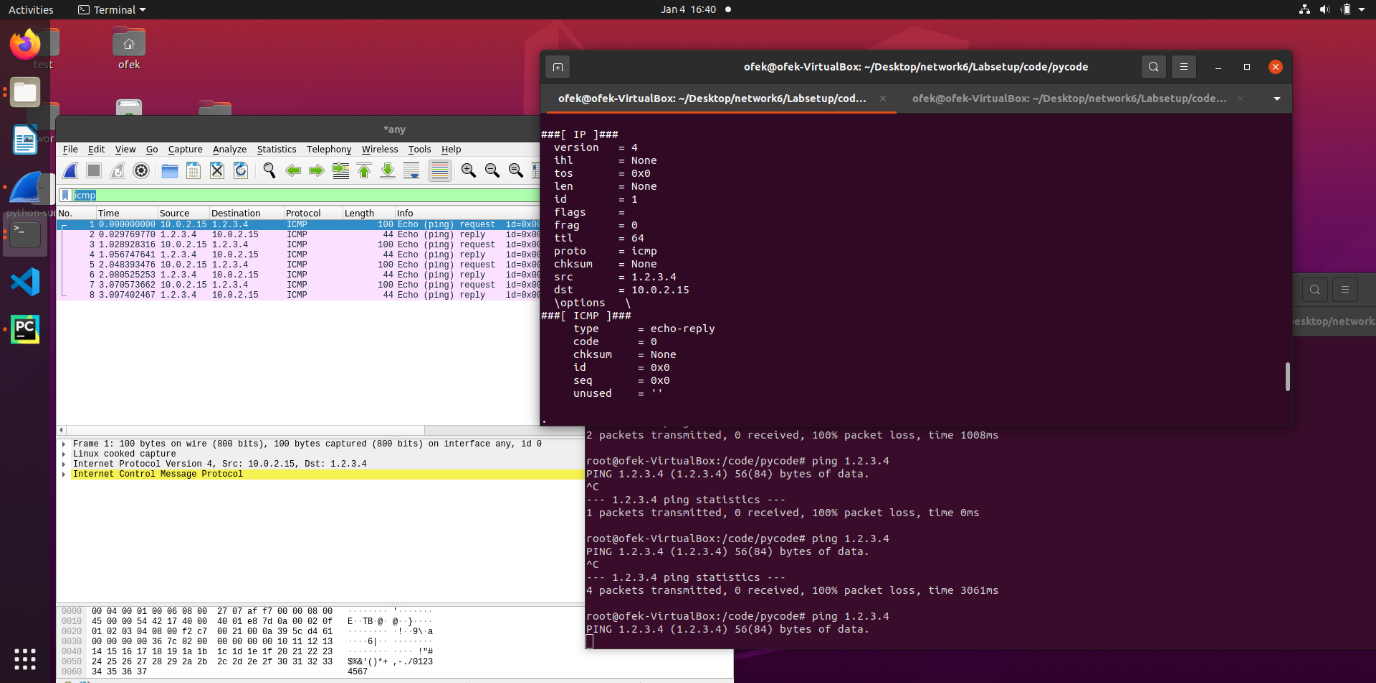
אפשר לראות שכTTL הוא 1 לא הגענו ליעד(פקטה צבועה בשחור בווירשארק) כך גם ל2 אבל ב4 כבר יש תשובה



1.4

סניף וספוף ל גוגל אכן שלחנו הודעה במקום גוגל 

סניף וספוף לכתובת חיצונית לא קיימת(1.2.3.4) מי שללח קיבל תשובה למרות שהכתובת אינה קיימת



2.1.A

אכן מצליחים להסניף באצמעות פיקאפ ניתן לראות מה קורה בווירשארק וראוים שאכן מקבלים תיאום עם המסניף של C

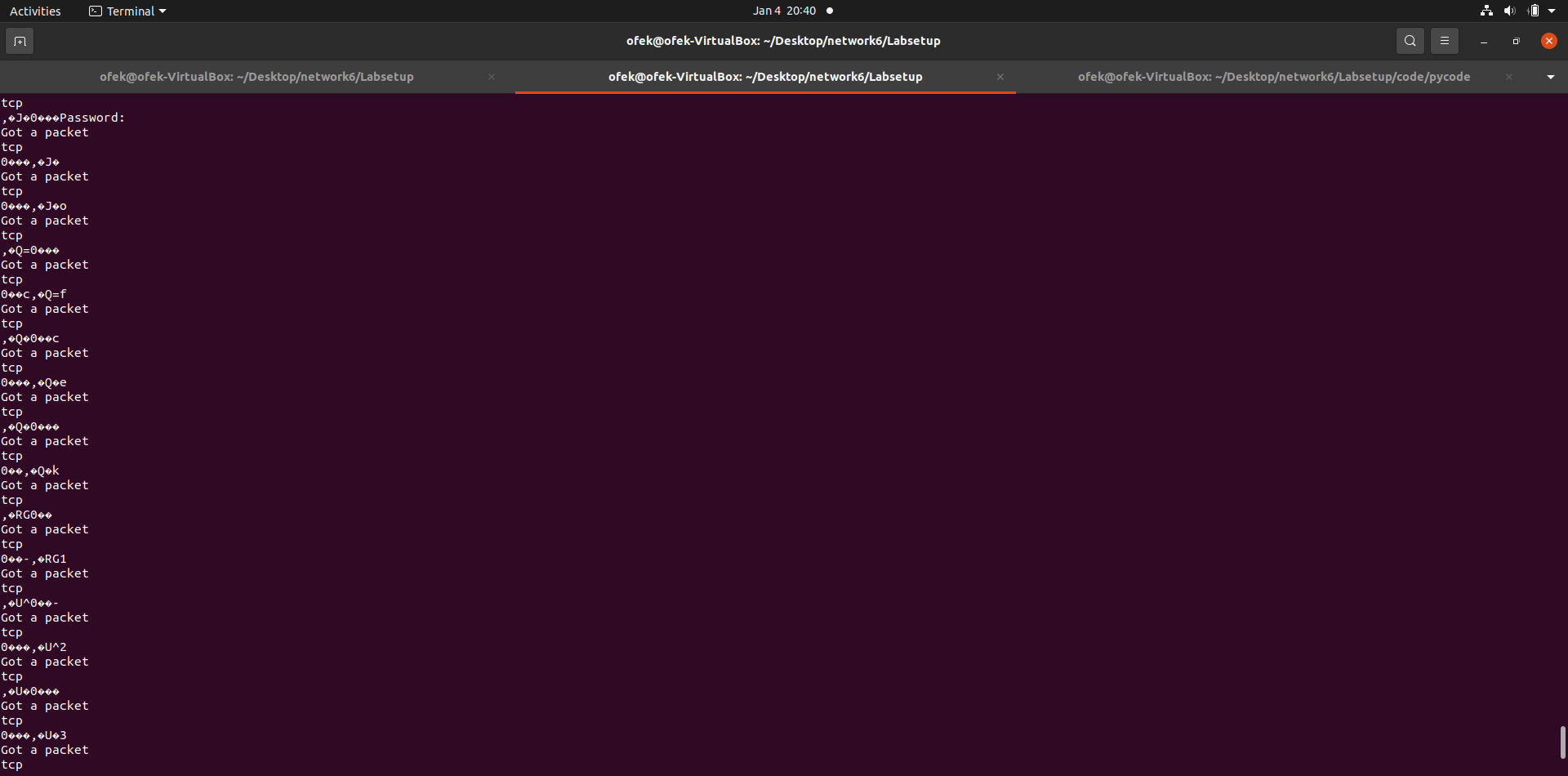
Graphical user interface, text

Description automatically generated

2.1.C

הסנפת סיסמאות בTELNET

הסנפת הסיסמאות של של התקשורת בTELNET את הסיסמא ניתן להפיק על ידי לקחת כל פקטה שנייה לאחר שרואים פקטה עם המילה פאסוורד ולקחת את האות האחרונה שלה כמו שניתן לראות פה הסיסמא היא ofek123 שזה אכן מה שהקלדתי, ההסבר לכך הוא שטלנט שולח אות אות עם גיבריש ביניהים

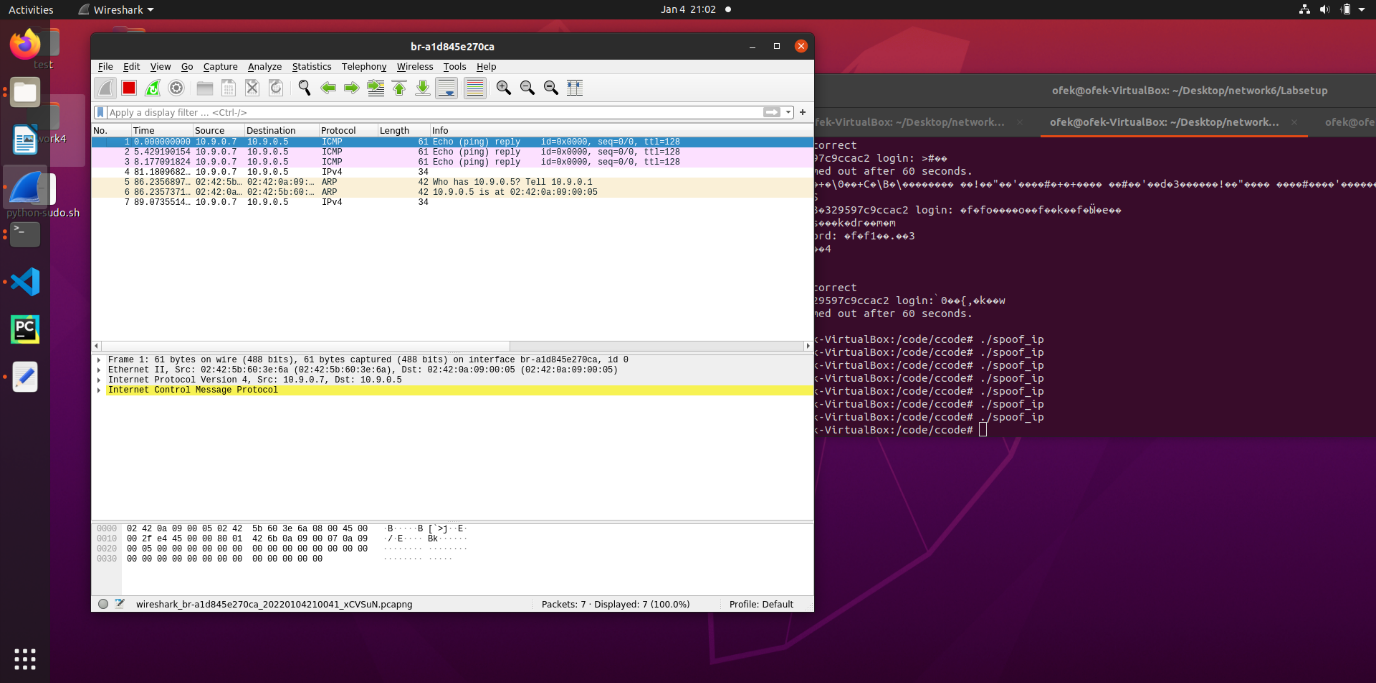
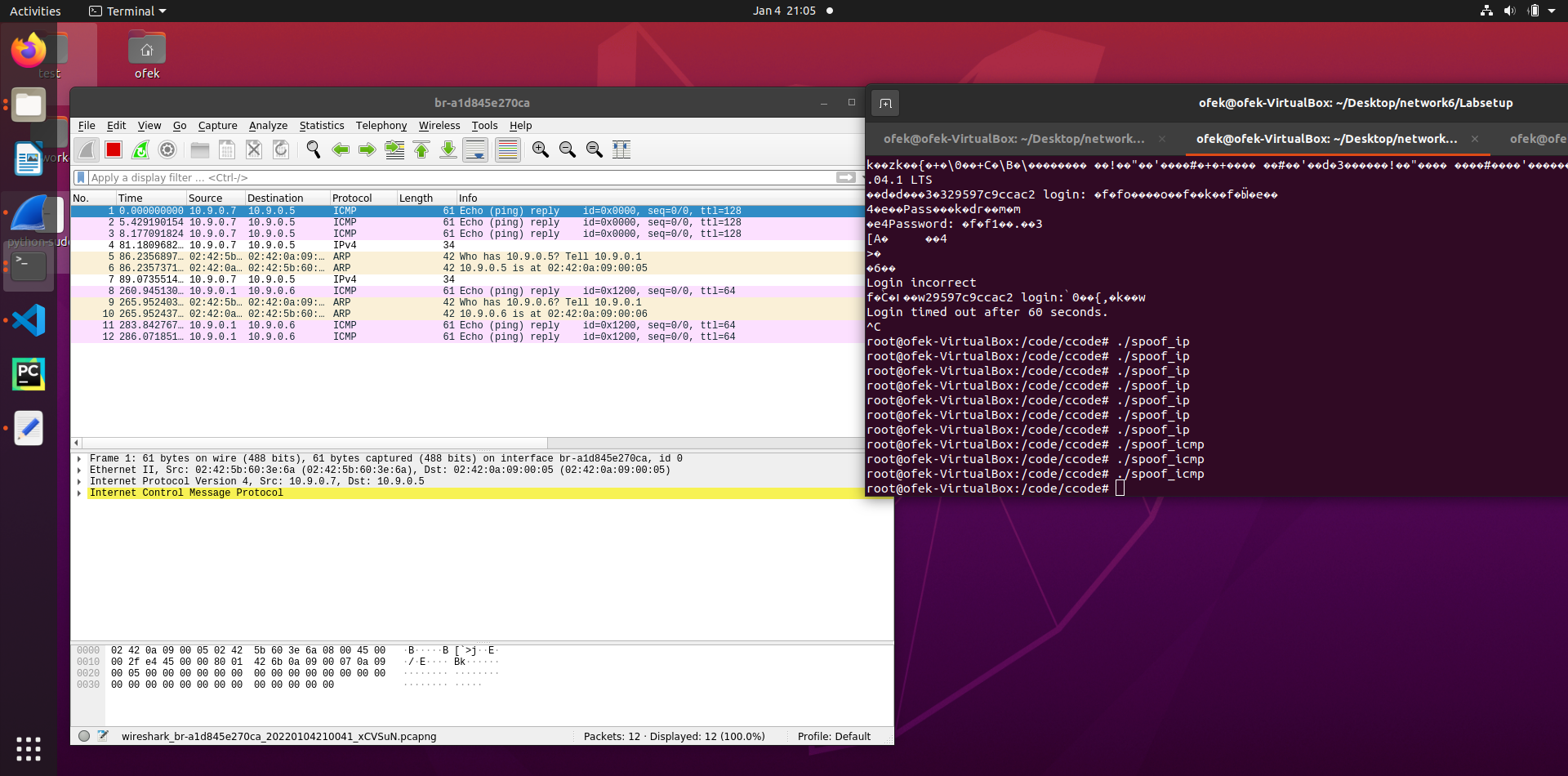




2.2.A.B

שלחתי פה שאלה מ 1.9.0.6 למרות שזו אינה הכתובת שלי וקיבלתי תשובה אליה (1.9.0.6 בעצם לא מצפה לתשובה)

בתמונה השנייה ניתן לראות זיוף של כתובת הIP SRC בפקטה של הIP על ידי



2.3

הסנפה וספופ לכתבות 1.2.3.4 כלומר פה שלחתי פינג לכתובת 1.2.3.4 שאינה קיימת הסנפתי אותה והחזרתי ריספונד לכתובת השולח ניתן לראות שזה אכן מה שקרה כי בווירשארק יש את כתובת 1.2.3.4 בבקשת ריספונד בתור המקור מה שלא יכול לקרות ללא ספופינג

