**תקשורת מחשבים**

**מטלה 2**

**מרצה**: עמית דביר.

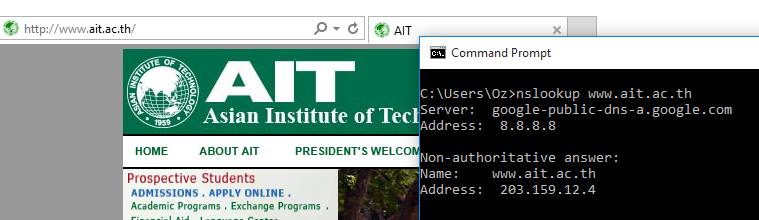
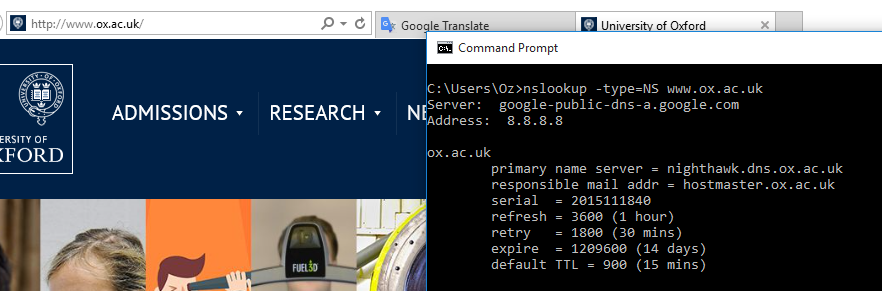
**מגישים**: עוז מעתוק 305181158,

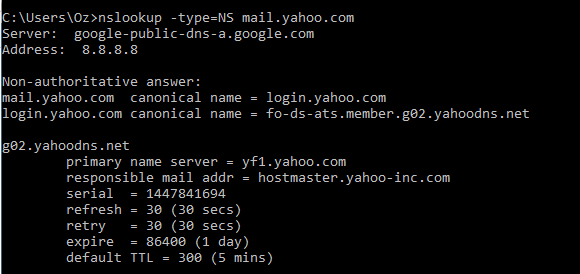
אבישלום ג'אן 308481423.

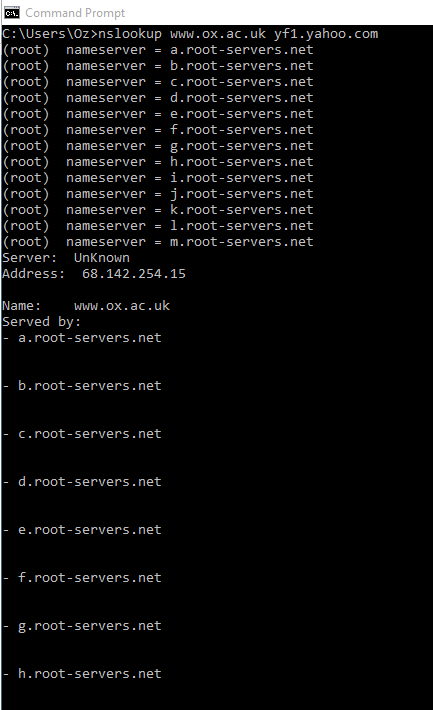
**חלק א' - Wireshark\_Intro\_v6.0.**

1. תשובה + תצלום מסך.
2. תשובה + תצלום מסך.
3. תשובה + תצלום מסך.

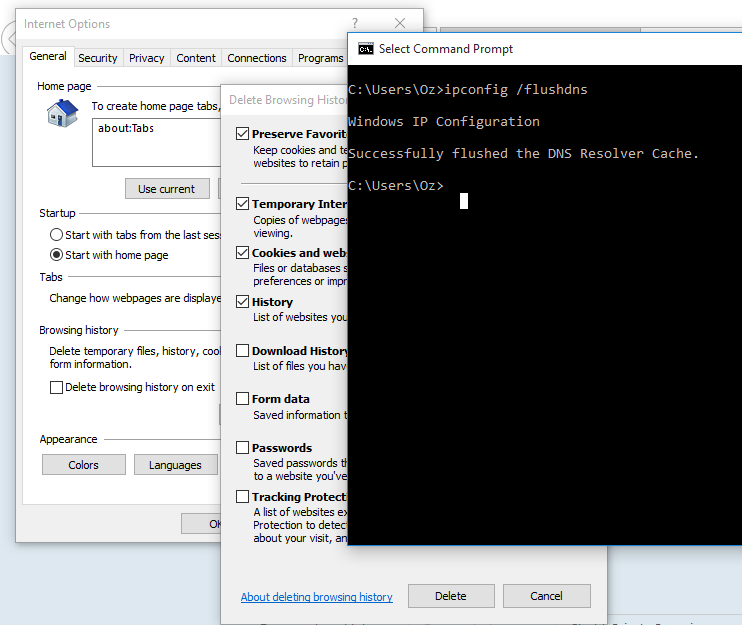
**חלק ב' - Wireshark\_DNS\_v6.01.**

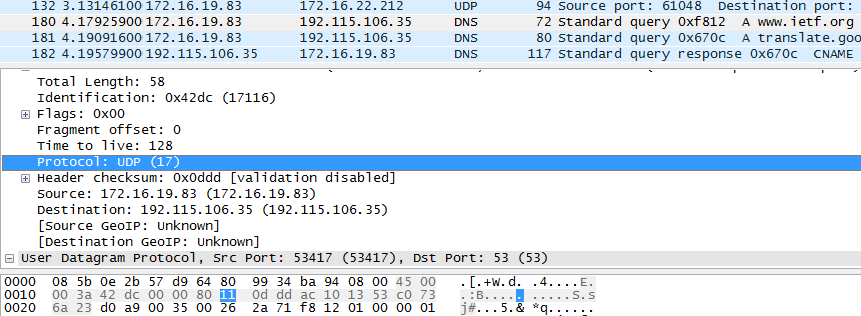
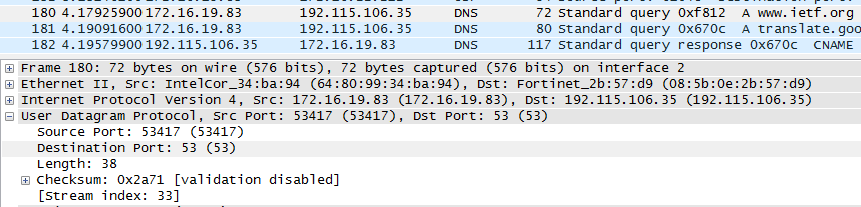
1. לאחר הרצת הפקודה nslookup ניתן לראות את השם כתובת ה – IP של האתר שביקשתי, ואת שם וכתובת ה – IP של שרת ה DNS אשר שירת אותי. 
2. חלר מהתשובה שאנו מקבלים ע"י הרצת הפקודה nslookup –type-NS כוללת את שם שרת ה – DNS המהימן עבור אותה כתובת שביקשתי.
3. נמצא את שם שרת ה DNS אשר מטפל עבורנו בבקשת האתר mail.yahoo.com , לאחר מכן נריץ את הפקודה nslookup עם שתי הכתובות. התשובה שאנו נקבל היא כלל שרתי ה – DNS אשר משרתים את האתרים הנ"ל.

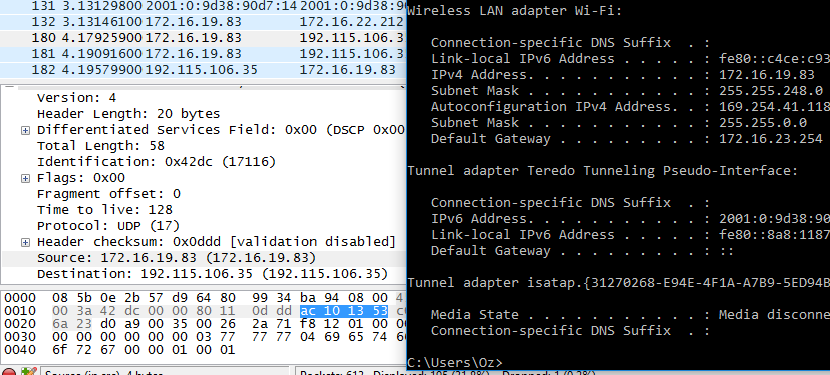




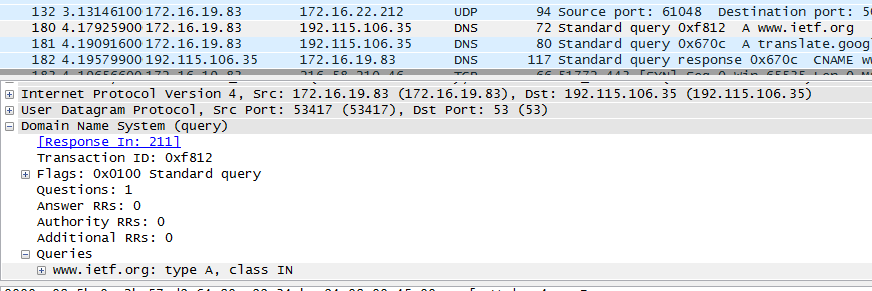
**הקרבה של ממש**



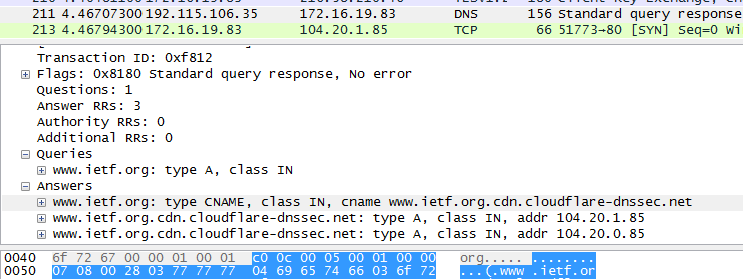
1. בפרטים אשר מציגה תוכנת ה wireshark ניתן לראות את נתוני החבילה ואיתם את הפרוטוקול בו עברה.
2. כתובות ה – des port & src port
3. כתובת ה – IP אשר אליה נשלחת הודעת ה DNS זהה לכתובת ה – IP של שרת ה – DNS ברירת המחדל שלי. (מפני שזה אותו שרת).



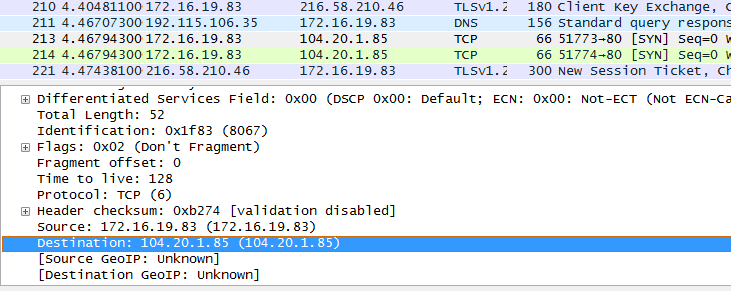
1. סוג הודעת ה – DNS הוא A. מוצגת גם לראות את שורת התשובות (בגלל שזה ההודעה שנשלחה, קיימת שאלה ולא תשובה בחבילה, בחבילה הבאה מוצג כי קיימת תשובה(.

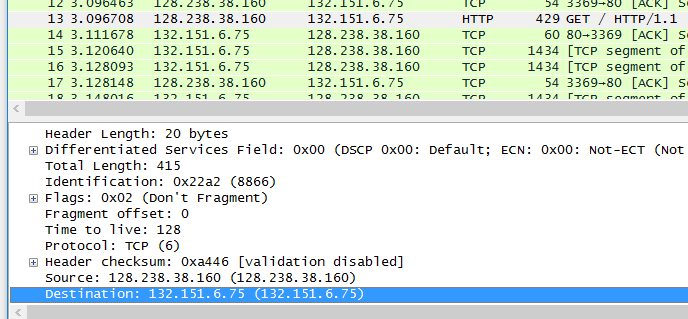


1. נמצא את התשובות לבקשת ה – DNS בחבילה הבאה, ובה מוצגים התשובות עבור דרישתנו.

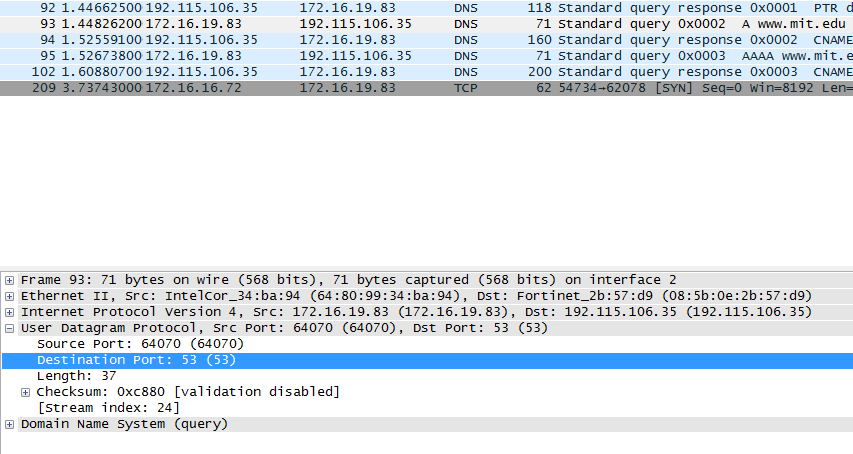


1. כתובת היעד של הודעת הסינכרון היא בעצם כתובת השרת שקיבלנו בתשובה בהודעת ה SYN

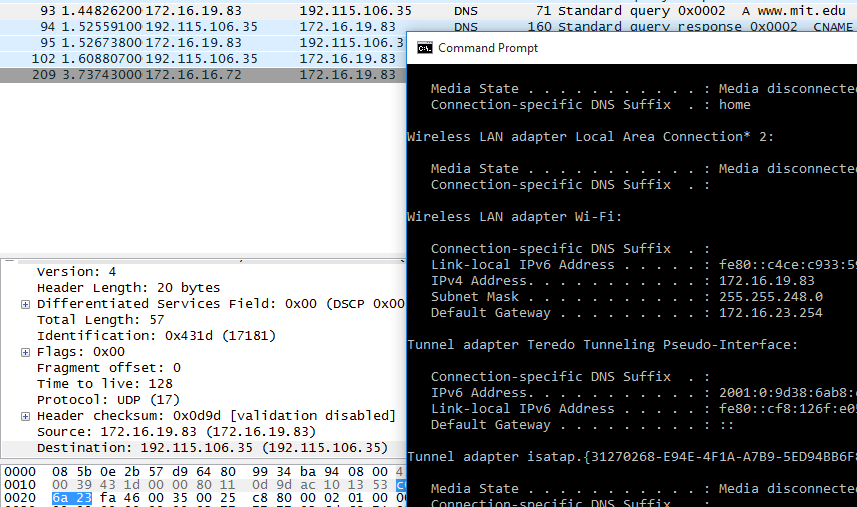


1. כאן השתמשנו בקובץ שצורף למסמך המעבדה (כי אצלנו לא נקלטו הודעות בקשה לתמונות), ניתן לראות את הודעת ה HTTP אשר מבקשת את התמונה. ההודעת כוללת כתובת יעד שאינה של שרת ה – DNS שביקשנו ממנו את האתר עצמו.

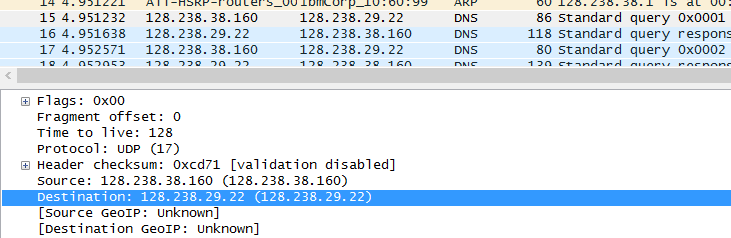
**נקליט את תעבורת הרשת שוב ב wireshark כאשר אנו מריצים את הפקודה - *nslookup* on** [**www.mit.edu**](http://www.mit.edu) **.**

בהקלטה נוכל לראות את חבילות ה – DNS שנשלחו בעקבות ביצוע הפקודה, כאשר גם פורט המקור וגם פורט היעד מופיעים

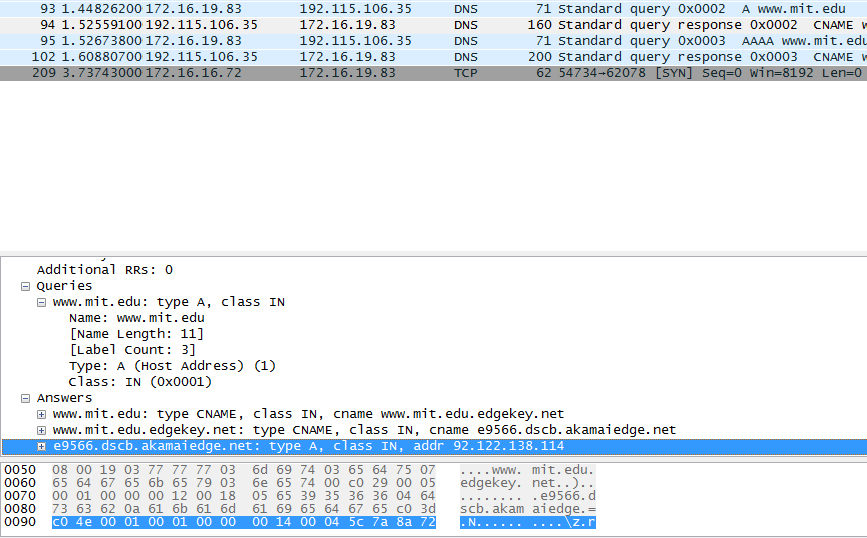
כתובת היעד של הודעות ה – DNS הוא כתובת שרת ברירת המחדל, בתמונה ניתן לראות את התשובה החוזרת משרת ברירת המחדל לכתובת שלי.



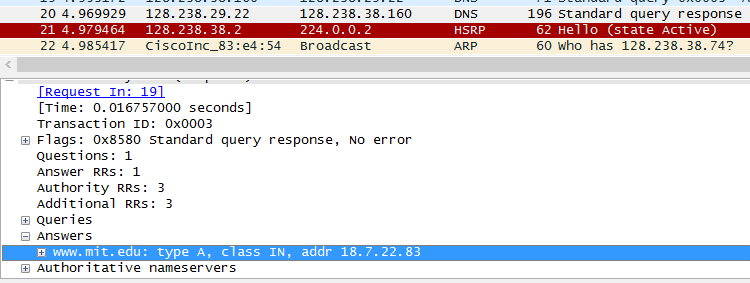
מצורף תמונת מסך מתוך קבצי ה pcap המקושרים במסמך המעבדה



1. סוג הודעת ה – DNS הוא A ושוב ניתן לראות את שורת התשובות מופיעה.



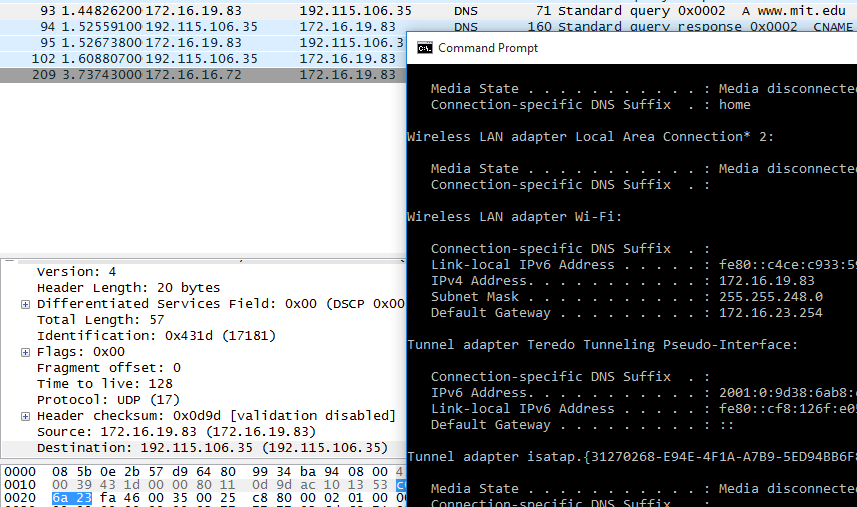
1. (שוב השתמשנו כאן בקבצי המעבדה), ניתן לראות את התגובה שמגיעה משרת ה – DNS הכוללת תשובה אחת ובה שם האתר, סוג ההודעה, וכתובת ה – IP של האתר.



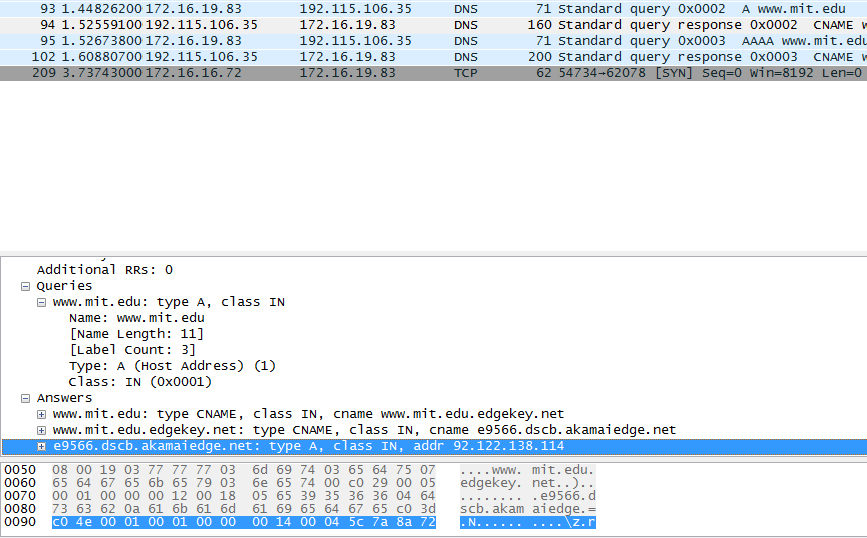
1. בום^^

**נקליט את תעבורת הרשת שוב ב wireshark כאשר אנו מריצים את הפקודה -** nslookup –type=NS mit.edu **.**

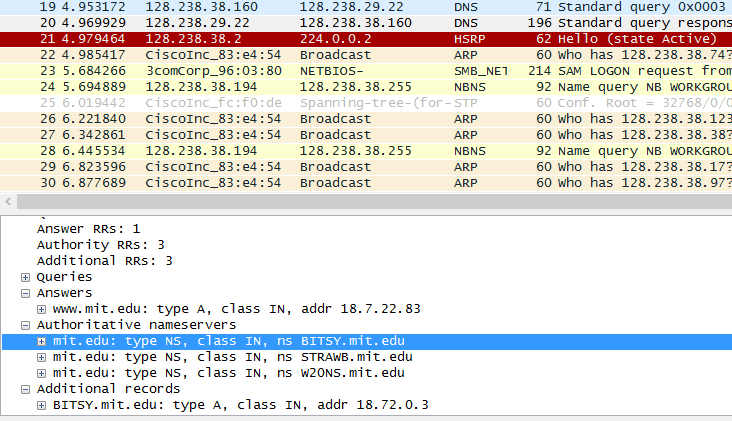
1. כתובת ה – IP אליה נשלחת הודעת ה – DNS זהה לכתובת ה – IP של שרת ברירת המחדל שלי.



1. סוג הודעת ה –DNS הוא A, והיתן לראות כי הוא מכיל 3 תשובות

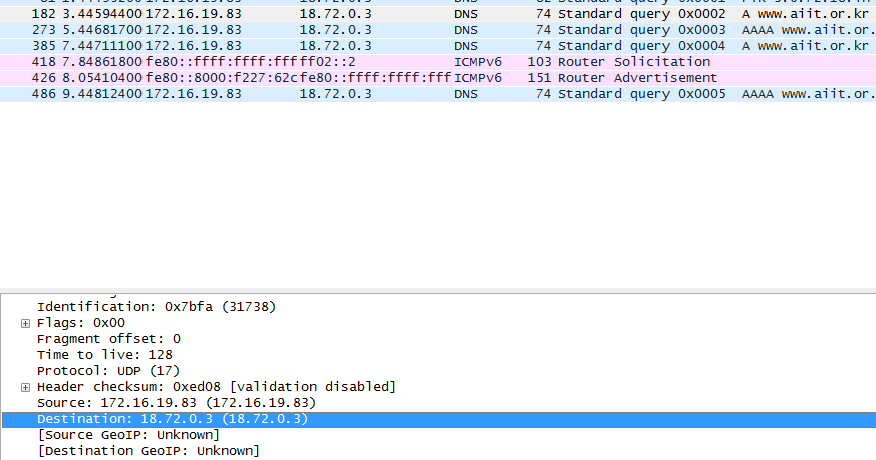


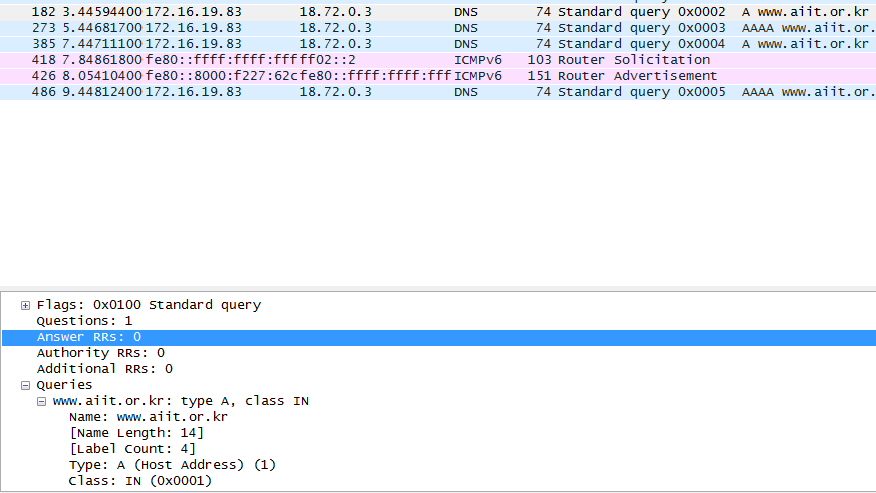
1. (קבצי המעבדה) בהודעת התגובה ניתן לראות שלושה תשובות הכוללות שם שרת ה MIT וכתובת ה – IP שלו.



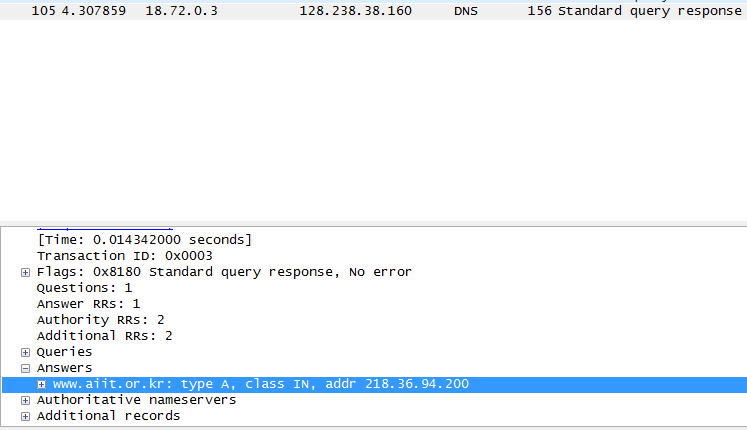
1. ^^

**נקליט את תעבורת הרשת שוב ב wireshark כאשר אנו מריצים את הפקודה -** nslookup www.aiit.or.kr bitsy.mit.edu **.**

1. בהודעת ה – DNS שנשלחת הפעם, ניתן לראות כי כתובת היעד איזה כבר שרת ברירת המחדל שלי, מפני שפקודה שהרצנו, הכנסנו אילוץ במסלול שליחת החבילה.(כתובת שרת ברירת המחדל שלי מופיע בשאלה 16). 
2. סוג הודעת ה – DNS הוא A וניתן לראות כי הוא אינו מכיל תשובות, מפני שזאת הודעת הבקשה.



1. (שוב תצלומי המסך הם מקבצי המעבדה) נראה כי בהודעת התגובה אנחנו מקבלים תשובה המכילה את שם האתר שביקשנו, סוג ההודעה, וכתובת ה – IP של האתר.



1. ^^