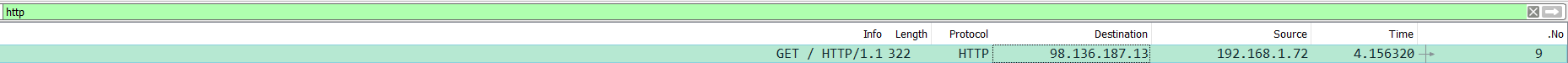
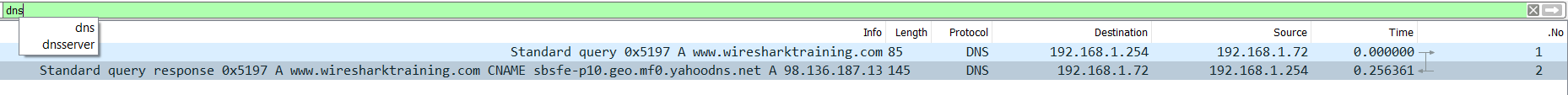
בס"ד

ישי לוטווק 304909864

**תשובות לתרגיל של השאלות על הwireshark**

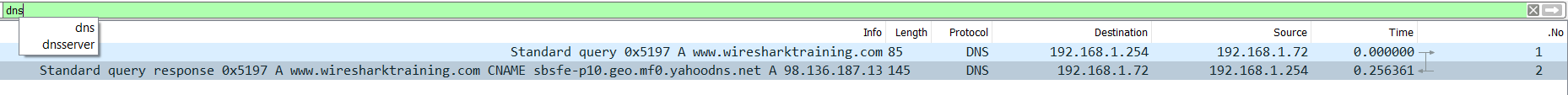
1. משני צילומי המסך ניתן להסיק כי כתובת הIP של הלקוח היא 192.168.1.72



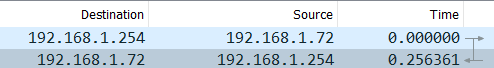


בצילום הראשון ניתן לראות שהלקוח פונה לשרת HTTP ובצילום השני ניתן לראות שהלקוח פונה לשרת DNS

2. ניתן לראות כי כתובת הIP של הDNS server היא 192.168.1.254



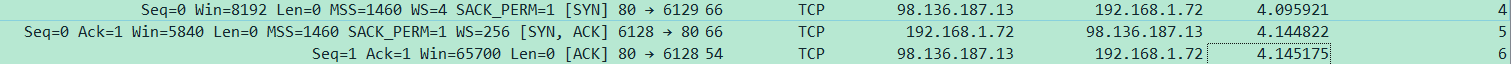
3. ניתן לראות כי זמן התגובה מרגע השליחה של הלקוח הוא בערך רבע שנייה.



4. ההסנפה יותר קרובה ללקוח.

כיון שאם נבחן את הודעות 4 ו5 נראה, שהזמן של המעבר של ההודעה הראשונה מרגע ההסנפה עד השליחה לשרת, ביחד עם הזמן של המעבר של ההודעה השנייה חזור מהשרת אל ההסנפה, היא בערך 0.05 שניות.

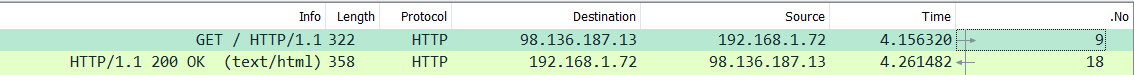
לעומת זאת, אם נבחן את הודעות 5 ו6 נראה, שהזמן של המעבר בין ההודעה השנייה מרגע ההסנפה עד לשליחה ללקוח, ביחד עם הזמן של המעבר של ההודעה השלישית חזור מהלקוח, היא בערך 0.001 שניות.



5. ניתן לראות כי כתובות הIP של שרתי הHTTP אליהם התחבר הלקוח בהצלחה הן:

98.136.187.13

98.139.206.151





6. השמות הם: [www.wiresharktraining.com](http://www.wiresharktraining.com)



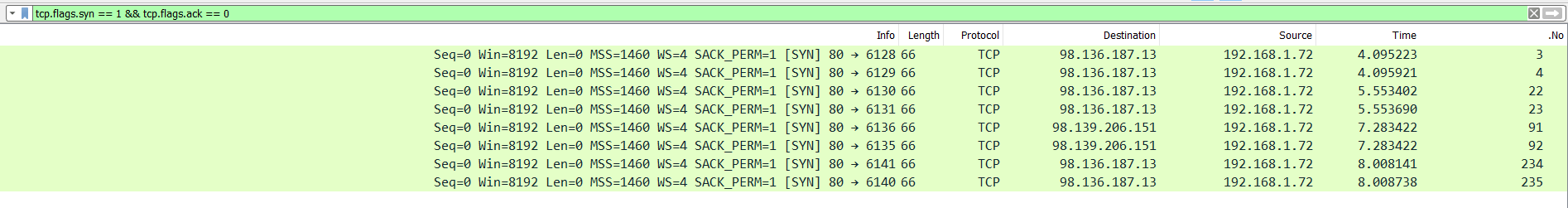
ו visit.webhosting.yahoo.com



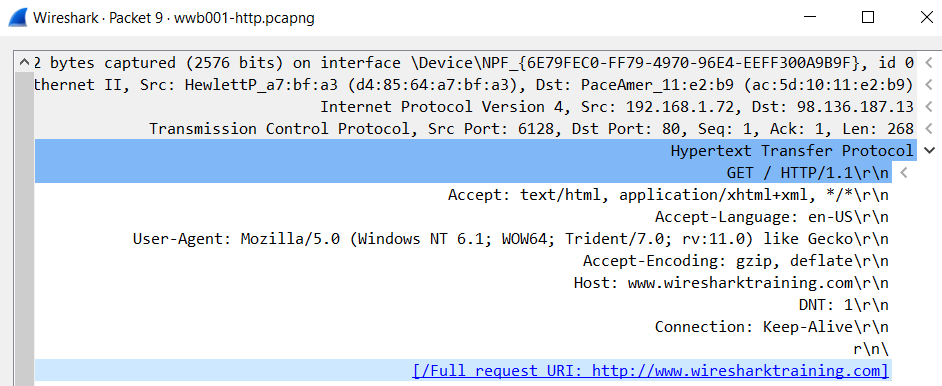
7. יש 8 פקטות כאלו.

ניתן למצוא אותן בקלות על ידי הכנסה של השורה הבאה לפילטור:

tcp.flags.syn == 1 && tcp.flags.ack == 0



8. ניתן לראות כי הבקשה הראשונה בURI היא: http://www.wiresharktraining.com

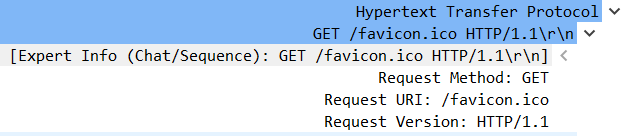


9. תגובת שרת עם סטטוס 404 שאומר שהבקשה לא נמצאה.



10. כפי שניתן לראות בבקשה לשרת האובייקט המבוקש הוא favicon.ico





11. ניתן לראות שמספרי הפורטים הם 6128, 6129, 6130, 6131, 6140, 6141

