מגישות:

זוהר שמחון 211871868

אנה פינצ'וק 206431082

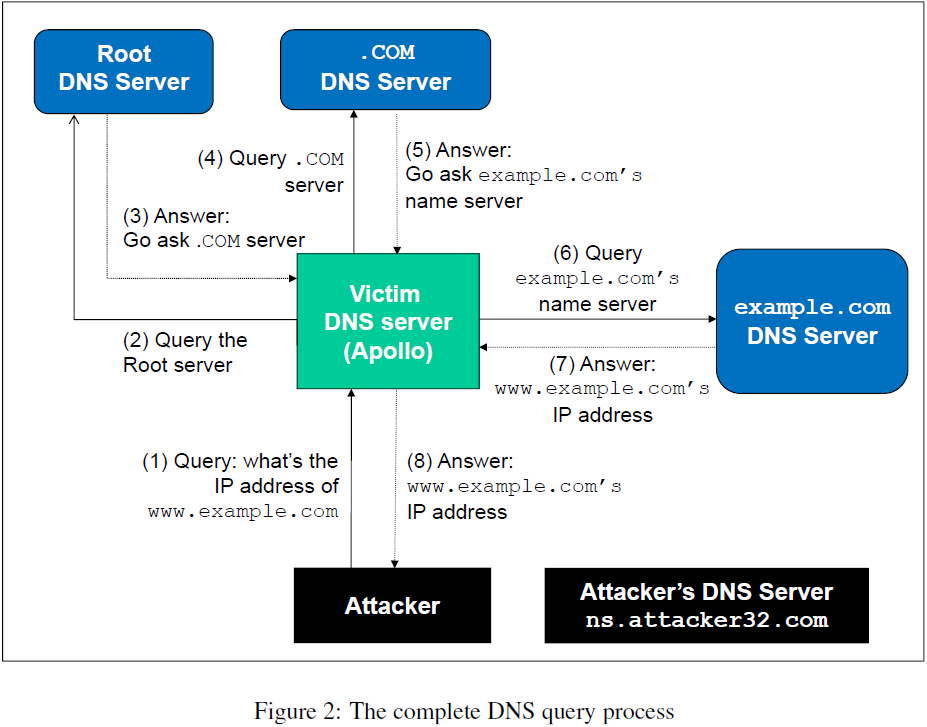
**הקדמה**:

במטלה זו היינו צריכים לבנות התקפת DNS Cache poisoning ששולחת בקשות ותשובות DNS לשרת DNS מקומי ממחשב התוקף לפורט 53 של השרת DNS. מטרתנו הייתה להידמות לNS שיש לו תשובה לגיטימית לבקשה שלנו ובמקום תשובה נכונה לשלוח לו כתובת של הNS של התוקף שבו כתובות לאתרים מזויפים כמו:www.example.con . זאת אומרת שכאשר משתמש יבקש את כתובת האתר, במקום הכתובת המקורית תינתן לו הכתובת המזויפת שנמצאת בNS של התוקף. כל זאת מתאפשר רק כאשר הקאש של השרת לא מכיל את הכתובת ולכן בכל איטרציה שינינו את השאילתה בכדי לוודא שאין את השאילתה בקאש.

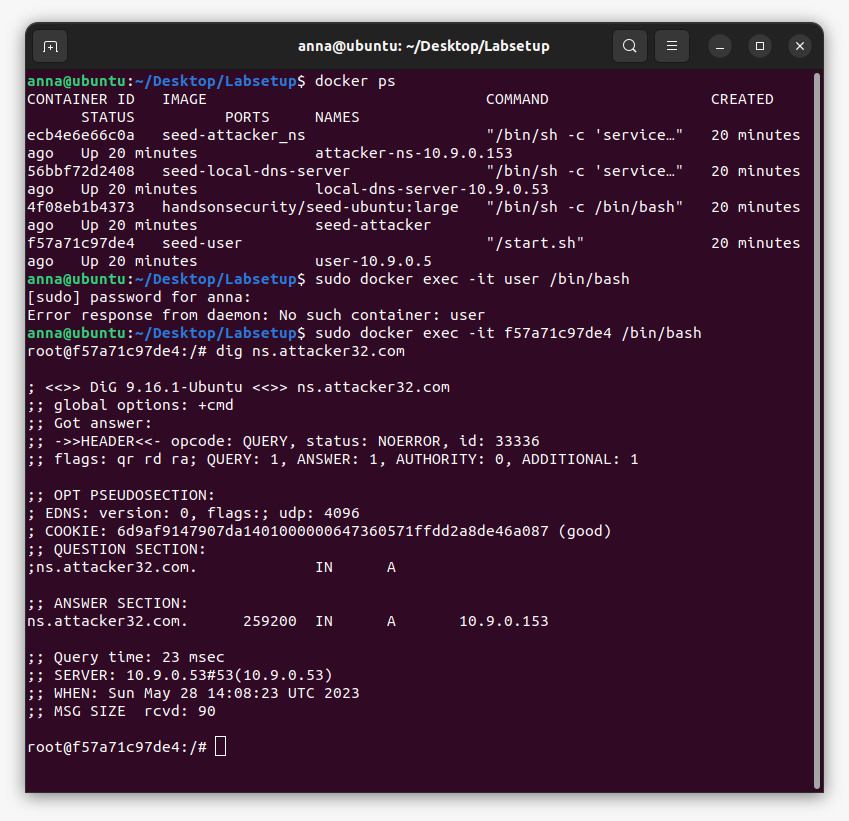
כתבנו את התוכנית בשתי שפות C ופייתון, בפייתון כתבנו את הבקשות והתשובות שכן יותר קל לבנות פקטות בפייתון, ולאחר מכן שמרנו אותם בקובץ, בשפת C פתחנו את הקבצים ושינינו את השדות המתאימים כיוון שלא היה הרבה לשנות. הרצנו שרת DNS ,משתמש,NS של תוקף, ותוקף על קונטיינרים נפרדים.

בכל התקפה נשלחה שאילתה אחת ואיתה לולאה של 500 פקטות עם ID שונה על מנת לנסות לעקוף את מנגנון ההגנה של שרת ה DNS שמצמיד ID לבקשה ולכן לתשובה אמור להיות אותו ID. כיוון שזהו מרוץ על זמן מי ייתן את התשובה מהר יותר אנחנו או הNS האחרים אנחנו מוותרים אחרי 500 פקטות ושואלים שאילתה חדשה כדי להרוויח שוב זמן.

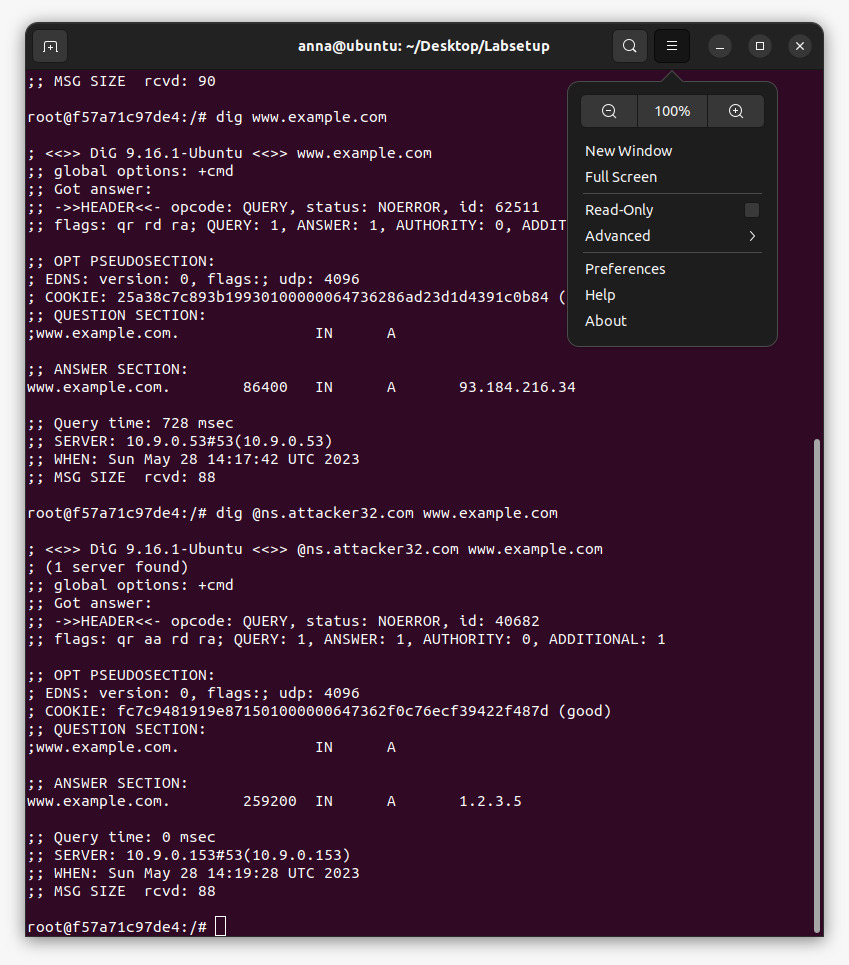
להלן איור שמתאר את ההתקפה:



תחילה התבקשנו לבצע את הפעולה הבאה: Get the IP address of **ns.attacker32.com**

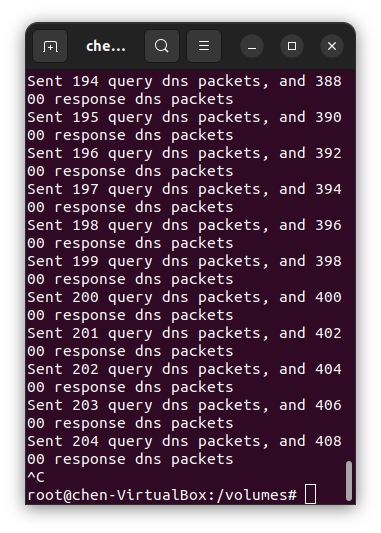


לאחר כשראינו שההכנות למעבדה הסתדרו כמו שצריך התבקשנו לבדוק מה התשובות שמקבל המשתמש לשאילתות הבאות:

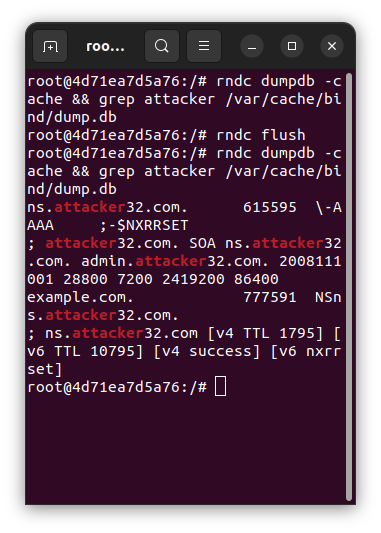


**מהלך ההתקפה:**

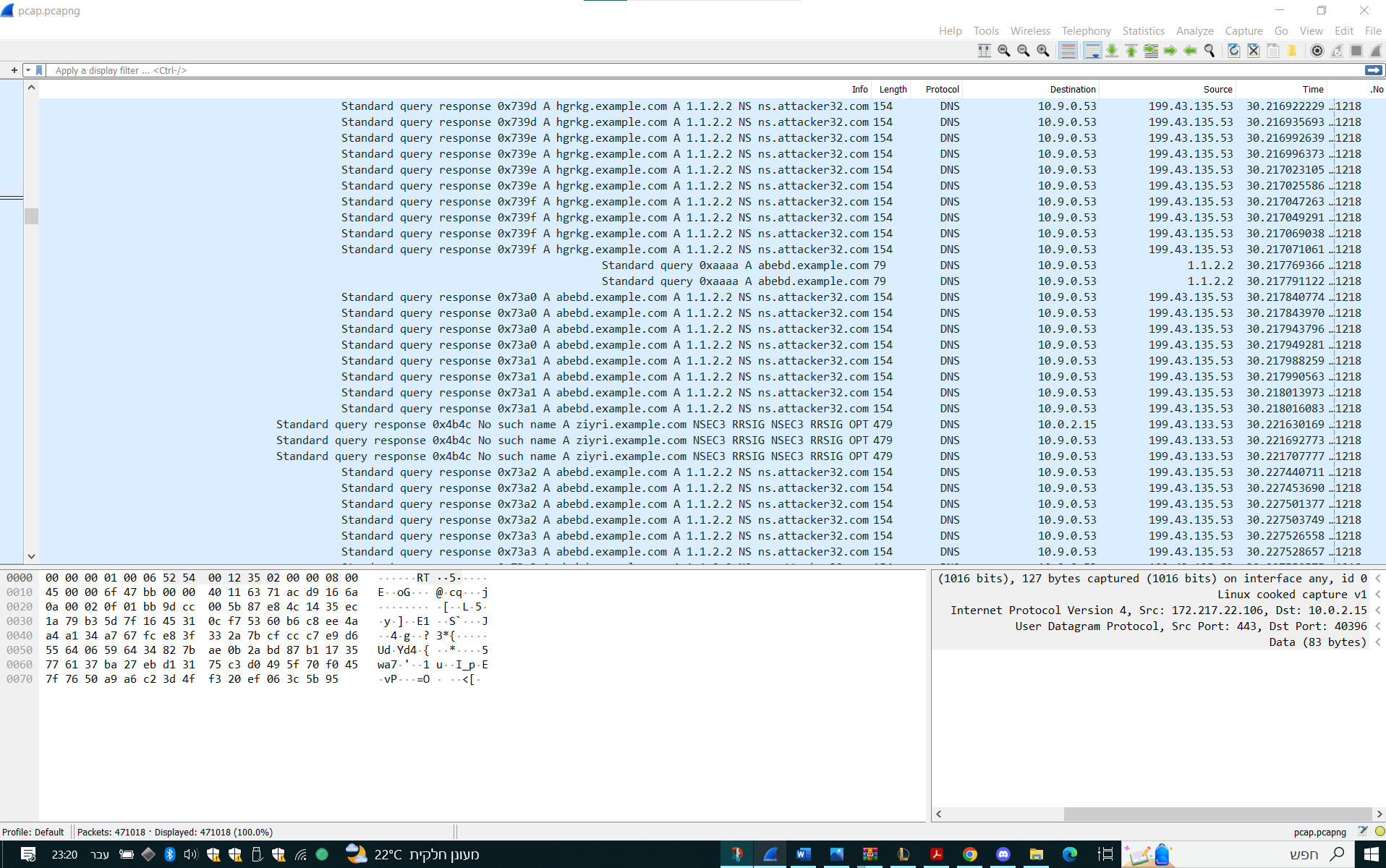
תחילה הרצנו את ההתקפה בדוקר של התוקף:



לאחר מכן ניקינו את הקאש של הDNS ובדקנו האם הוא השתנה להכיל את מה שההתקפה שלחה לו:



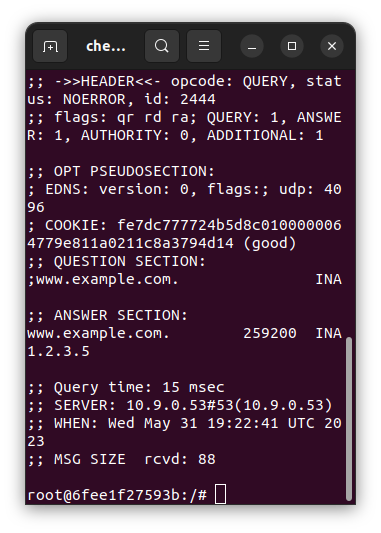
כפי שניתן לראות בתיעוד מתוכנת ה wireshark שלהלן ההתקפה הצליחה וכל הפיצ'רים שעשינו אכן מופיעים בפירוט הפקטות(שינוי שאילתה,שינוי ID , שינוי תשובות):



**תוצאות:**

ניתן לראות שכאשר אנחנו שואלים את המשתמש את השאילתה: dig ns.attacker32.com

הוא מציג לנו את הכתובת של התוקף:



ואכן ניתן לראות שזוהי הכתובת שנמצאת בNS של התוקף כמו שהראנו בתחילת הדו"ח.

**מסקנות:**

לפי הממצאים שלנו ניתן לזייף בקלות שאילתות ותשובות DNS על מנת להתחזות לכתובות קיימות על שרתי DNS לא מוגנים. לכן מומלץ להשתמש בשרתי DNS מורשים ומוגנים.