**דוח חלק ב**

שרת DNS לא אוטורטיבי:

בהתחלה עשינו nslookup ל-meta, קבלנו את התעבורה הבאה:

Graphical user interface, text, application

Description automatically generated

בשורה 7 ניתן לראות את הפניה לשרת הdns שהגדרנו, לאחר מכן נשים לב שהוא פונה לגוגל (עם כתובות בipv6), בשורות 5-6,8-11, ואז בשורה 13 השרת dns המקומי מחזיר את התשובה שקיבל מגוגל.

כעת הרצנו שוב nslookup ל-meta, וקבלנו את התעבורה הבאה: Graphical user interface, text, application, email

Description automatically generated

נשים לב שהפעם כמו קודם בשורה 1, אנו פונים לשרת dns המקומי, אך הפעם שמור לא כבר בcache הכתובת של meta ולכן הוא לא פונה לגוגל וישר מחזיר לנו תשובה בשורה 2.

הסבר על השדות בפרוטוקול DNS:

בקשת הDNS:

Graphical user interface, text, application, email

Description automatically generated

נעבור על השדות:

Graphical user interface, text, application

Description automatically generatedכלומר מספר השאילתות-1

נכנס לשאילתה,

Graphical user interface, text, application, email

Description automatically generated

ניתן לראות שמבקשים את כתובת הIPv4 לפיGraphical user interface, text, application, email

Description automatically generated, של הdomain: Graphical user interface, text, application, email

Description automatically generated

תשובת הDNS:

Graphical user interface, text, application

Description automatically generated

נעבור על השדות:

נשים לב שהID זהה-Graphical user interface, text, application

Description automatically generated

יש תשובה אחת-Graphical user interface, text, application

Description automatically generated

כעת נשים לב שהשאלה שעליה הוא ענה היא מה ה-IP של meta, כלומר ענה לשאלה שלנו:

Graphical user interface, text, application, email

Description automatically generated

בנוסף ניתן לראות שאכן היא ה-IP.

**חלק שני – שרת DNS אוטורטיבי**

בשלב זה הגדרנו את שרת ה DNS להיות שרת אוטורטיבי – הגדרנו לשרת קובץ שיכיל את הניהול של הדומיין biu.ac.il וכן הגדרנו רשומות מתאימות שימפו לנו בין דומיינים מסוימים לכתובת ה ip של המחשב שלנו.

נדגים עבור כל אחת מהרשומות שהשרת אכן עונה את התשובות הנכונות בהתאם לרשומות שהגדרנו בקובץ.

**רשומת NS**

ברשומה זו מיפינו בין שרת השמות של הדומיין biu.ac.il לבין ה ip של המחשב שלנו, כפי שניתן לראות בתיעוד הבא:

תמונה שמכילה טקסט, כתום, צילום מסך, הגדר

התיאור נוצר באופן אוטומטי

**תצלום 2.1 : מיפוי בין שרת השמות של biu.ac.il לכתובת ה-ip של המחשב**

נראה כיצד הדבר מתבטא בתעבורה שהוסנפה ע"י wireshark:



כאמור, ניתן לראות פניית DNS מסוג NS לשרת האוטורטיבי שהקמנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כעת, אם נסתכל על התשובה שהשרת מחזיר, נשים לב שהוא מחזיר את ה ip של המחשב שלנו – ולא את של שרת השמות האמיתי. זאת כאמור כפי שרצינו, והגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

נשים לב שאף התבצע A על מנת לדעת את כתובת ה ip של שרת השמות (כפי שציפינו), עבורה מופתה כתובת הip של המחשב שלנו – כפי שהגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**רשומת MX**

ברשומה זו מיפינו בין השרת המשמש את הדומיין biu.ac.il לקבלה של דואר אלקטרוני לבין ה ip של המחשב שלנו, כפי שניתן לראות בתיעוד הבא:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**תצלום 2.2 : מיפוי בין שרת הדואל של biu.ac.il לכתובת ה-ip של המחשב**

נראה כיצד הדבר מתבטא בתעבורה שהוסנפה ע"י wireshark:



כאמור, ניתן לראות פניית DNS מסוג MX לשרת האוטורטיבי שהקמנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כעת, אם נסתכל על התשובה שהשרת מחזיר, נשים לב שהוא מחזיר את ה ip של המחשב שלנו – ולא את של שרת הדואל האמיתי. זאת כאמור כפי שרצינו, והגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

נשים לב שאף התבצע A על מנת לדעת את כתובת ה ip של שרת הדואל (כפי שציפינו), עבורה מופתה כתובת הip של המחשב שלנו – כפי שהגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**רשומת A**

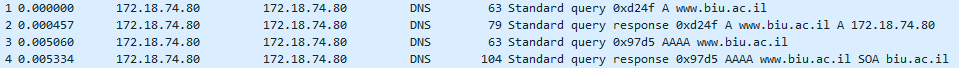
ברשומה זו מיפינו בין השרת המשמש את הדומיין www.biu.ac.il לבין ה ip של המחשב שלנו, כפי שניתן לראות בתיעוד הבא:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**תצלום 2.3 : מיפוי בין שרת הדואל של biu.ac.il לכתובת ה-ip של המחשב**

נראה כיצד הדבר מתבטא בתעבורה שהוסנפה ע"י wireshark:



כאמור, ניתן לראות פניית DNS מסוג A לשרת האוטורטיבי שהקמנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

כעת, אם נסתכל על התשובה שהשרת מחזיר, נשים לב שהוא מחזיר את ה ip של המחשב שלנו – ולא את של שרת הדואל האמיתי. זאת כאמור כפי שרצינו, והגדרנו ברשומות:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

עוד נוכל לשים לב, כי התבצעה אף בקשת AAAA לזיהוי כתובת בגרסה ipv6

אם נשים לב טוב יותר, נוכל לראות כי השרת מחזיר תשובת SOA (start of authority) – רשומה שמצביעה על המצאותו של ה zone.

אכן, בתשובה השרת מחזיר את הפרטים שהיו כתובים ברשומת ה SOA שהגדרנו:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

**בדיקת הcache:**

בהתחלה היה בקאש רק את meta שחיפשנו קודם לכן:

Text

Description automatically generated

אחר כך הרצנו שוב, הפעם עם mako וראינו שה-IP נוסף לקאש:

Text

Description automatically generated