שיעור 5 – DNS  
**תרגיל: Look Up!**

בתרגיל זה נכיר את הכלי nslookup ונלמד לעבוד איתו. כרגיל ניעזר בהסנפות כדי להבין מה קורה מאחורי הקלעים.

הוראות שימוש לפקודת nslookup:

|  |  |
| --- | --- |
| בקשה רגילה - רשומת A (מהשרת המוגדר במחשב) | nslookup yahoo.com |
| בקשה רגילה משרת DNS לבחירתי (בדוגמא זו 8.8.8.8) | nslookup yahoo.com 8.8.8.8 |
| בקשה של רשומה מסוג שהוא לא A | nslookup –type=NS yahoo.com |

**1. שימוש ב-nslookup**

1. בעזרת הפקודהnslookup, בקשו את ה-IP של אתר yahoo.com. כתבו את הפקודה שכתבתם:

|  |
| --- |
| nslookup yahoo.com |
| תשובה |

1. מהי כתובת ה-IP של יאהו שקיבלתם? מהי כתובת ה-IP של שרת ה-DNS שענה לכם?

|  |
| --- |
| 74.6.143.25 yahoo. 10.100.102.1. שרת שענה לי |
| תשובה |

1. בעזרת שימוש ב-type כמו בדוגמא למעלה, בקשו את הכתובות של **שרתי הדואר** (MX) של yahoo.com. כתבו את הפקודה:

|  |
| --- |
| nslookup -type=MX yahoo.com |
| תשובה |

1. בקשו את ה-IP של אתר yahoo.com משרת DNS אחר מזה שהשתמשתם בו עד עכשיו  
   (חפשו בגוגל Public DNS Servers). כתבו את הפקודה:

|  |
| --- |
| nslookup yahoo.com 8.8.8.8 |
| תשובה |

**2. הסנפת DNS**

1. התחילו הסנפה ב-Wireshark. בזמן שההסנפה מתבצעת, היכנסו לשני אתרים לבחירתכם בדפדפן.
2. כעת עצרו את ההסנפה.
3. כתבו פילטר אשר מציג רק את בקשות ה-DNS שנשלחו **ממחשבכם** (חבילות יוצאות).

|  |
| --- |
| dns && ip.src == 10.100.102.84 |
| תשובה |

1. מהו הפורט של פרוטוקול DNS? איפה אתם רואים את זה בהסנפה?

|  |
| --- |
| 53, בחלון האמצעי, בשכבה האחת לפני האחרונה (בהנחה ששכבת האפליקציה היא האחרונה). (אולי שכבת הקו?) |
| תשובה |

1. כתבו כמה בקשות מופיעות לאחר ביצוע הפילטר (היעזרו ב-Displayed שמוצג בתחתית התוכנה).

|  |
| --- |
| 217 |
| תשובה |

1. בחרו את אחת מבקשות ה-DNS וסמנו אותה במסך העליון של Wireshark. במסך האמצעי, סמנו את השורה התחתונה ביותר אשר נקראת Domain Name System (query).
2. תארו איזה מידע מסומן כעת בכחול בחלק התחתון של Wireshark. האם המידע הזה קריא? הסבירו מדוע.

|  |
| --- |
| מסומן גם הhex שלא קריא וגם התרגום שלו לאנגלית שאפשר לקרוא |
| תשובה |

1. כעת עברו לסינון**dns** כדי להציג את כל הבקשות והתשובות יחד. בחרו את אחד **מבקשות ה-**DNS.
2. במסך התחתון, לחצו פעמיים על השורה התחתונה Domain Name System (query). כעת אנו יכולים לצפות במידע שנכלל בפרוטוקול DNS בצורה מסודרת ונוחה (Wireshark מתרגם את המידע הבינארי עבורנו).
3. אחד השדות בפרוטקול הוא מזהה השיחה מזהה השיחה (Transaction ID). מה הערך שלו?

|  |
| --- |
| 0x4c5b |
| תשובה |

1. הרחיבו את שדה ה-Flags (דגלים). אלו שדות של 0 או 1. איך אפשר לדעת לפי הדגלים עם ההודעה היא בקשה או תגובה?

|  |
| --- |
| בדגל הראשון כתוב ההודעה היא <בקשה או תגובה> אפשר גם לדעת כי 0 זה שאלה ו 1 זה תשובה |
| תשובה |

1. כמה בקשות מופיעות תחת שדה Queries ולאילו דומיינים? מה הסוג של כל בקשה (A/MX/NS...)

|  |
| --- |
| 1. לדומיין שביקשנו. סוג A |
| תשובה |

1. בתחתית המידע על DNS, מופיע קישור הכחול אשר מוביל לתשובה שנשלחה לבקשה זו. לחצו עליו לחיצה כפולה. האם החבילה שמסומנת במסך העליון השתנתה בעת הלחיצה? מהי החבילה שמסומנת כעת לדעתכם? מהו ה-Transaction ID בחבילה הנוכחית?

|  |
| --- |
| כן החבילה המסומנת השתנתה. התשובה לבקשה. אותו ID - 0x4c5b |
| תשובה |

1. כעת אחרי השדה של Queries התווסף לנו שדה נוסף – Answers. מהו ה-IP של הדומיין המבוקש?

|  |
| --- |
| video-api.yql.yahoo.com |
| תשובה |

1. בתוך התשובה מופיע גם שדה בשם Time to Live. מהו הערך שבו? מה מייצג הערך? אם אינכם יודעים, היעזרו בגוגל.

|  |
| --- |
| 257, כמה קפיצות hops נשאר לחבילה לעשות לפני שהיא תהרוג את עצמה. זה קיים בשביל למנוע לופ אינסופי שהחבילה תעבור, בפקודה tracert משתמשים בטיים טו ליב קטן שעולה באחד אחד כדי לחשוף את כל הקפיצות |
| תשובה |

**3. קבלת תשובה מוסמכת**

**תשובה מוסמכת (Authoritative)** היא תשובה אשר מגיעה היישר משרת ה-DNS של חברת האחסון של האתר. שרתים אלו מכונים "מוסמכים" מכיוון שהם המקור הכי אמין לקבל כתובת של אתר.  
למשל, אם אני רוצה לקבל תשובה מוסמכת לגבי ה-IP של yahoo, עלי לפנות ישירות לשרת ה-DNS של יאהו ולשאול אותו (במקום לשאול את השרת המקומי שלי).

1. חפשו את ה-IP של אתר אוני' בן גוריון bgu.ac.il (אין צורך בהסנפה בסעיף זה).
2. קראו את מה שכתוב בפלט של nslookup בתשומת לב. האם התשובה אותה קיבלתם היא תשובה מוסמכת (Authoritative)? אם לא, הסבירו מדוע לא? מאיפה לדעתכם הגיעה התשובה?
3. נסו להשיג תשובה **מוסמכת** לאתר bgu.ac.il. לשם כך נצטרך לברר מיהו שרת ה-DNS ה-Authoritative של bgu.ac.il (רמז: חזרו לסוגי רשומות במצגת השיעור). תארו את כל מה שעשיתם כדי לקבל תשובה מוסמכת:

|  |
| --- |
| לא הצלחתי |
| הקש תשובה |

1. ns1.yahoo.com הוא השרת ה-Authoritative של אתר Yahoo. נסו לבקש ממנו את הכתובת לאתר bgu.ac.il. תארו את התשובה, והסבירו מדוע קיבלתם אותה לדעתכם.

|  |
| --- |
| קיבלתי תשובה מוסמכת כי ביקשתי את הIP מהשרת הרשמי של יאהו. לכן הוא לא כתב שזה תשובה לא מוסמכת. ובסרוור היה כתוב את השם של הסרוור ומתחתיו את האיי פי שלו. |
| הקש תשובה |

**4. מתשאלים את מערכת ה-DNS העולמית בעצמנו!**

**כדי לענות על חלק זה, עליכם ללמוד את מצגת ההרחבה של שיעור זה – היררכיית ה-DNS**

בתרגיל זה תמלאו את התפקיד שלרוב ממלא עבורנו שרת ה-DNS של ספק האינטרנט, והוא להתרוצץ במורד היררכיית ה-DNS כדי לקבל תשובה מוסמכת!

עליכם לגלות את כתובת ה-IP של הדומיין google.com. היעזרו בכלי nslookup ובצעו את השלבים הבאים:

1. בחרו בשרת Root כלשהו. כתבו מהי כתובת ה-IP שלו והיכן מצאתם אותה?

|  |
| --- |
| לא הצלחתי |
| הקש תשובה |

1. באמצעות תשאול שרת ה-Root, גלו מיהו שרת ה-TLD האחראי על ה-Zone של .com מיהו שרת ה-TLD? מהי כתובת ה-IP שלו? כתבו את הפקודה שכתבתם.

|  |
| --- |
| לא הצלחתי |
| הקש תשובה |

1. באמצעות שרת ה-TLD האחראי על ה-Zone של .com, גלו מיהו השרת האחראי על google (ה-Authoritative שלו). כתבו את הפקודה שכתבתם.

|  |
| --- |
| לא הצלחתי |
| הקש תשובה |

1. באמצעות השרת ה-Authoritative של google, גלו מהי הכתובת של google.com, וכתבו אותה פה. כתבו את הפקודה שכתבתם.

|  |
| --- |
| 216.58.210.46 |
| הקש תשובה |

1. נסו להקיש את הכתובת בשורת הכתובת ב-Chrome. אם נטען האתר של גוגל – הצלחתם!