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. הסנפת DNS**

1. התחילו הסנפה חדשה ב-Wireshark, ופתחו cmd.
2. בעזרת הפקודהnslookup, בקשו את ה-IP של אתר yahoo.com. כתבו את הפקודה שכתבתם:

|  |
| --- |
| באופן הפשוט ביותר ניתן לחפש כך:  nslookup yahoo.com |
| הקש תשובה |

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

|  |
| --- |
| כתובת של יאהו:  כתובת של השרת DNS שענה לי: |
| הקש 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 |
| הקש תשובה |

1. בקשו את ה-IP של אתר yahoo.com משרת ה-DNS החופשי של גוגל (8.8.8.8). כתבו את הפקודה:

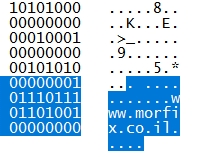
|  |
| --- |
| nslookup yahoo.com 8.8.8.8 |
| הקש תשובה |

1. כעת עצרו את ההסנפה.
2. כתבו פילטר אשר מציגרק את בקשות ה-DNS שנשלחו **ממחשבכם** (חבילות יוצאות).

|  |
| --- |
| פילטר אפשרי הוא:  dns and ip.src=<my\_ip>  או  udp.dstport == 53 (אבל את זה לא למדנו ממש עדיין) |
| הקש תשובה |

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

|  |
| --- |
|  |
| הקש 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.

מרבית המידע לא קריא (מוצג כנקודות) מכיוון שהפרוטוקול DNS **אינו טקסטואלי**. יש בו חלקים טקסטואלים, למשל איפה שכתובת כתובת האתר, אך מרביתו אינו טקסטואלי. זה לא אומר שלא עובר בו מידע או שהוא לא קריא בכלל, פשוט צריך עזרה בפירוש שלו ע"י תוכנה. Wireshark עוזרת לנו בכך שהיא מציגה לנו את הנתונים בצורה פשוטה.

1. כעת עברו לסינון**dns** כדי להציג את כל הבקשות והתשובות יחד.
2. כעת לחצו על החץ **<** שמופיע משמאל ל-Domain Name System (query). כעת אנו יכולים לצפות במידע שנכלל בפרוטוקול DNS בצורה מסודרת ונוחה (Wireshark מתרגם את המידע הבינארי עבורנו, במקום שאנחנו נעשה זאת בעצמו כפי שעשינו בתרגיל "כסף מלוכלך").
3. כתבו את הערך של מזהה השיחה (Transaction ID)

|  |
| --- |
|  |
| הקש תשובה |

1. הרחיבו את שדה ה-Flags (דגלים) וכתבו את כל המידע שאתם יכולים להבין על הבקשה משדה זה.

|  |
| --- |
| לפרוטוקולים רבים יש שדה flags שמאפשר לסמן לצד השני פרטים לגבי ההודעה. במקרה של DNS ישנם דגלים שונים המאפשרים להגיד האם מדובר בבקשה או תגובה, האם אנחנו דורשים שהחיפוש יהיה רקורסיבי, האם אנחנו מוכנים לקבל בקשות לא מוסמכות ועוד. |
| הקש תשובה |

1. כמה בקשות מופיעות תחת שדה Queries?

|  |
| --- |
| במקרה הזה שלחנו כל פעם בקשה אחת ולכן תהיה בקשה אחת בלבד. |
| הקש 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?

|  |
| --- |
| מדובר באותו Transaction ID, וככה המחשב שלנו יודע להצמיד את התשובה שהתקבלה לבקשה ששלחנו (יכול להיות ששלחנו מספר בקשות, ובדרך הזו אנחנו יכולים בקלות לדעת איזו תשובה מתאימה לאיזו בקשה). |
| הקש תשובה |

1. מצאו את שדה ה-Time to Live אשר מופיע בתשובה. מהו הערך שבו? מה מייצג הערך? אם אינכם יודעים, היעזרו בגוגל.

|  |
| --- |
| אם ניכנס לתוך רשומת A ספציפית שחזרה אלינו בתשובה, נראה שדה Time To Live עם מספר יחסית גדול (לא להתבלבל עם שדה ה-TTL של פרוטוקול IP שנמצא במקום אחר בחבילה – נלמד עליו בהמשך הקורס).  שדה ה-TTL אומר לנו כמה זמן בשניות עלינו לשמור את התשובה הזאת עד שהתוקף שלה פג (אז נצטרך לשלוח בקשה מחדש כי אנחנו כבר לא יכולים לסמוך על כך שכתובת ה-IP של הדומיין לא השתנתה). הנתון הזה נשמר ברשומת ה-A של שרת ה-DNS שמכיל את הרשומה הרלוונטית, ומי שאחראי על השרת מגדיר אותו.  עבור דומיינים שכתובת ה-IP שלהם נשארת יחסית קבועה, ה-TTL יהיה גבוה. לעומת זאת, דומיינים שיש חשש שה-IP שלהם ישתנה יגדירו TTL נמוך יותר... |
| הקש תשובה |

**2. קבלת תשובה מוסמכת**

1. חפשו את ה-IP של אתר אוני' בן גוריון bgu.ac.il (אין צורך בהסנפה בסעיף זה).
2. האם התשובה אותה קיבלתם היא תשובה מוסמכת (אשר מגיעה מהשרת ה-Authoritative)? אם לא, הסבירו מדוע לא? מאיפה לדעתכם הגיעה התשובה?

|  |
| --- |
| הסיכוי הסביר הוא שקיבלתם תשובה לא מוסמכת. זה קורה כי שרת ה-DNS הלוקאלי שלכם הוא לא שרת ה-DNS שמחזיק את הרשומות NS של אוניברסיטת בן גוריון, והוא כנראה מחזיר לכם תשובה מה-cache שלו. ניתן לקרוא עוד על כך בקישור הזה לדוגמה:  http://serverfault.com/questions/413124/dns-nslookup-what-is-the-meaning-of-the-non-authoritative-answer |
| הקש תשובה |

1. נסו להשיג תשובה מוסמכת לאתר bgu.ac.il. הסבירו כיצד הצלחתם ומה היתה הפקודה או הפקודות ששלחתם:

|  |
| --- |
| כדי לקבל תשובה מוסמכת, אנחנו צריכים לתשאל את שרת ה-DNS שמחזיק את הרשומות (שרת ה-DNS של אוניברסיטת בן גוריון). חיפוש באינטרנט יכול לעזור לנו להבין שניתן לתשאל את שרת ה-DNS שלנו לגבי מיהו שרת ה-DNS האותורטיבי המתאים (לדוגמה ניתן למצוא הסבר כאן - <https://support.rackspace.com/how-to/nslookup-checking-dns-records-on-windows/>).  נשתמש בפקודה –type=soa או  (גם זה יעבוד - -type=NS)  ונזהה ששרת ה-DNS האותורטיבי הוא dns2.bgu.ac.il, למשל. ועכשיו ניתן לפנות אליו ישירות ע"י פקודה כזאת:  nslookup bgu.ac.il dns2.bgu.ac.il  ונקבל תשובה מוסמכת! |
| 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.

|  |
| --- |
| אנו מקבלים תשובה של Query Refused. זה מכיוון שהשרת ה-Authoritative של יאהו לא אמור לענות על בקשות של אתרים שלא קשורים אליו! הוא לא שרת של ספק אינטרנט. |
| הקש תשובה |

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

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:

בחרו בשרת Root כלשהו. איך מצאתם את ה-IP? מהי כתובת ה-IP שלו?

|  |
| --- |
| כתובות ה-IP של שרת ה-root מוכרים לכולם, אחרת שרתי ה-DNS לא היו יודעים איפה להתחיל... בדוגמה הזאת נשתמש בכתובת 198.41.0.4, אותה ניתן למצוא באינטרנט (כמו שאר הכתובות).  דרך נוספת כי פשוט לחפש את רשומות ה-NS של הדומיין הכללי (".") באופן הבא:  nslookup –type=NS . |
| 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?

|  |
| --- |
| אוקיי אז התשאול הנ"ל נתן לנו את שרת ה-ROOT שאנחנו רוצים לתשאל אותו. עכשיו אנחנו יכולים לשאול אותו למי יש את הרשומה של google.com, שזה שרת ה-TLD שמעניין אותנו!  נרשום את הפקודה הבאה:  nslookup google.com 198.41.0.4  נקבל תשובה מאוד ארוכה, אבל כל החלק הראשון שלה זה רק רשימת השרתים שענו לנו.  אם נגלול למטה נראה את התשובות הרבות:  Name: google.com  Served by:  - a.gtld-servers.net  192.5.6.30  - b.gtld-servers.net  192.33.14.30  כל השרתים שקיבלנו הם שרתי TLD (רואים לפי הכתובת שלהם) שמטפלים ב-.com. אם נחפש אתר של .ninja נקבל שרתים אחרים לגמרי.  פקודה נוספת שיכלנו להריץ היא  nslookup –type=NS com. 198.41.0.4  שימו לב שחיפשנו את “com.” ולא את “com” – במידה וחיפשתם בלי הנקודה, יכול להיות שדיפולטית קיבלתם את שרתי ה-TLD של “il” כי אנחנו פונים מישראל... |
| הקש תשובה |

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

|  |
| --- |
| שוב, פשוט נבחר את אחד משרתי ה-TLD שקיבלנו ונחפש את google כמו שעשינו עד עכשיו:  nslookup google.com 192.5.6.30  ונקבל את שרתי ה-DNS ה-Authoritative של גוגל. |
| הקש תשובה |

1. באמצעות השרת ה-Authoritative של google, גלו מהי הכתובת של maps.google.com, וכתבו אותה פה.

|  |
| --- |
| עכשיו עלינו סוף סוף לבצע בקשת שאיננה בקשת NS, כי אנחנו מעוניינים ברשומת ה-A של שרת ה-DNS אליו אנחנו פונים!  nslookup google.com 216.239.34.10  פקודה זו תיתן לנו בשעה טובה את כתובות ה-IP שמתאימות לדומיין אותו חיפשנו. כתובת לדוגמה (יכול להיות שהכתובות יהיו שונות עבורכם במידה וגוגל משנים את הכתובות שלהם):  128.139.200.50 |
| הקש תשובה |

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