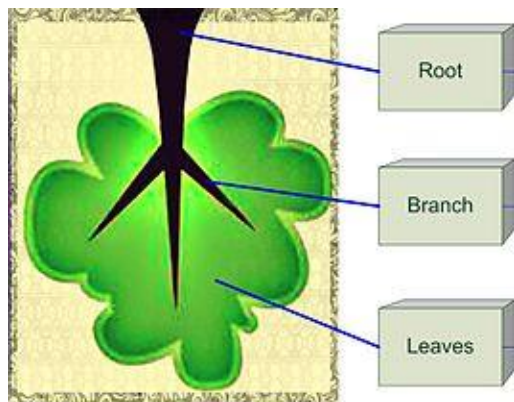


DNS



עקבו אחרי ההוראות שבתרגיל.
לאורך הדרך עליכם למלא 3 טבלאות.
העלו למודל מסמך word ובו שלשת הטבלאות (מלאות)
ולצד כל טבלה תמונה של הרשומה מ wireshark
שלפתם את הנתונים
לסיום כתבו את שם האתר שחיפשתם ואת הכתובת שלו
והוסיפו את תמונת הרשומה ממנה שלפתם את הכתובת

1 הרצת שאילתת DNS

1.1 הרצת השאילתה

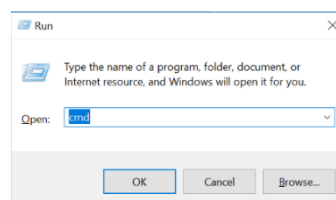
ניזכר בפקודה nslookup, אותה למדנו במבוא. פקודה זו פונה ל DNS server בשאילתות

1. פתחו את wireshark מתוך סביבת גבהים
2. כוונו אותו להסנפה עם filter לפרוטוקול dns
3. פתחו חלון command line
לחצו על מקש החלונות + R

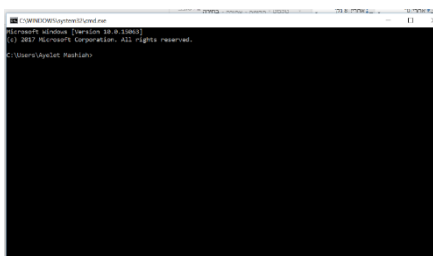


+ R

כתוצאה יפתח חלון ההרצה:



כתבו cmd ולחצו enter

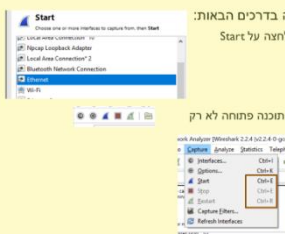


4. התחילו הסנפה. הכניסו כפילטר dns

הסנפה – START, STOP, RESTART

ניתן להתחיל, לעצור או להתחיל מחדש הסנפה בדרכים הבאות:

- דרך הקיצור במסך הפתיחה – בחירת interface נלחצה על Start
- דרך הכפתור בסרגל הכלים העליון, בכל שלב בו התוכנה פתוחה לא רק במסך הפתיחה:
- דרך התפריט Capture → (start, Stop, Restart)
- יש גם קיצור מקלדת Ctrl + E
- Ctrl + R



5. כתבו בחלון ה command line nslookup www.google.com

```

Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Ayelet Mashiah>nslookup www.google.com
Server: Unknown
Address: 10.0.0.138

Non-authoritative answer:
Name:    www.google.com
Addresses: 2a00:1450:400c:c04::67
          74.125.206.99
          74.125.206.105
          74.125.206.147
          74.125.206.104
          74.125.206.106
          74.125.206.103

C:\Users\Ayelet Mashiah>

```

עיצרו את ההסנפה

1.2 מבנה השאילתה

נסתכל ברשומת השאילתה:

93: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 II, Src: LiteonTe_52:a4:d1 (c8:ff:28:52:a4:d1), Dst: Netgear_13:fb:b6 (20:4e:7f:13:fb:b6)
 Internet Protocol Version 4, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.138 (10.0.0.138)
 User Datagram Protocol, Src Port: 59647 (59647), Dst Port: domain (53)
 Domain Name System (query)
 [Response In: 94]
 Transaction ID: 0x0002
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries

מלאו את הטבלה הבאה על פי ההסנפה שלכם:

שדה	ערך
Transaction ID	
Flags	
Questions	
Answer RRS	
Authority RRS	
Additional RRS	

מלאו את
הטבלה והוסיפו
תמונה במסמך
המענה

הסבר

Transaction ID – נועד לזיהוי התשובה (ל query ולתשובה יש אותו transaction ID)

Flags – משקפים את טיב השאילתה

Questions – מספר ה queries ב Transaction - יכולות להישלח מספר queries. בתמונה למעלה יש

אחת

RRS – Resource Records רשומות מסוגים שונים שהפרוטוקול מעביר בתוכן את האינפורמציה

1.3 Queries

מלאו את הטבלה על פי ההסנפה שלכם

Queries
 + www.google.com: type A, class IN

שדה	ערך
type	
class	

הסבר
 A – שאילתה לתרגום Domain Name
 ל IP
 IN – סוג הרשת בה אנחנו משתמשים
 intelligent network

מלאו את
הטבלה והוסיפו
תמונה במסמך
המענה

ראינו שהשאלתה שלנו היא שאלתה מסוג A. פתחן שוב הסנפה והריצו בחלון ה Command line את הפקודה:

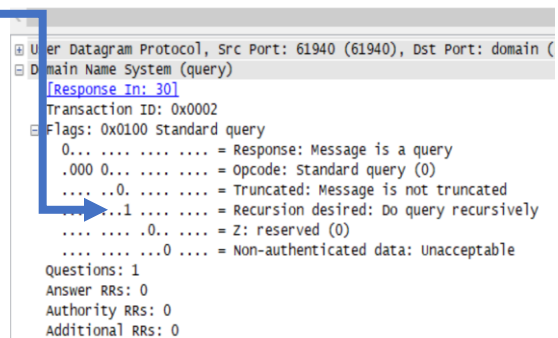
Nslookup 8.8.8.8

של מי הכתובת הזו?
 כבו את ההסנפה ובידקו מהו סוג ה Query?

הסבר: סוג ה query המבקש לתרגם IP ל Domain name נקרא PTR

1.4 flags

נשים לב ל flag – RD – recursion
 Desired. מה מבקש המחשב שלנו
 תשובה חלקית או תשובה על כל ה
 Domain name?



```

User Datagram Protocol, Src Port: 61940 (61940), Dst Port: domain (53)
Domain Name System (query)
  [Response in: 30]
  Transaction ID: 0x0002
  Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    ... ..0... .. = Truncated: Message is not truncated
    ... ..1... .. = Recursion desired: Do query recursively
    ... ..0... .. = Z: reserved (0)
    ... ..0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  
```

בידקו בשכבת ה IP בהודעה (Internet Protocol) את ה IP של היעד. של מי ה IP הזה?
 זוהי כתובת ה IP של שרת ה DNS. מיהו לדעתכם שירת זה?
 פתחו חלון ה command line והריצו את הפקודה **ipconfig**. האם אתם מוצאים את השרת.

Answer 2

פתחו שוב הסנפה והריצו בחלון ה command line שוב את הפקודה nslookup www.google.com

הפעם נבדוק את התשובה:

```

29 21.019700 10.0.0.4 10.0.0.138 DNS 74 Standard query 0x0002 A www.google.com
30 21.024625 10.0.0.138 10.0.0.4 DNS 90 Standard query response 0x0002 A www.google.com A 216.58.213.228
31 21.027517 10.0.0.4 10.0.0.138 DNS 74 Standard query 0x0003 AAAA www.google.com AAAA 2a00:1450:4005:
32 21.038320 10.0.0.138 10.0.0.4 DNS 102 Standard query response 0x0003 AAAA www.google.com AAAA 2a00:1450:4005:

<
Frame 30: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: Netgear_13:fb:b6 (20:4e:7f:13:fb:b6), Dst: LiteonTe_52:a4:d1 (c8:ff:28:52:a4:d1)
Internet Protocol Version 4, Src: 10.0.0.138 (10.0.0.138), Dst: 10.0.0.4 (10.0.0.4)
User Datagram Protocol, Src Port: domain (53), Dst Port: 61940 (61940)
Domain Name System (response)
[Request In: 29]
[Time: 0.004925000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers

```

מלאו את הטבלה הבאה על פי ההסנפה שלכם:

שדה	ערך
Transaction ID	
Flags	
Questions	
Answer RRS	
Authority RRS	
Additional RRS	

מלאו את
הטבלה והוסיפו
תמונה במסמך
המענה

הסבר

Transaction ID – נועד לזיהוי התשובה (ל query ולתשובה יש אותו transaction ID)

❖ השוו את ה Transaction ID לזה שבחבילת ה query/

Flags – משקפים את טיב התשובה

Questions – מספר ה queries ב Transaction - יכולות להישלח מספר queries.

RRS – Resource Records רשומות מסוגים שונים שהפרוטוקול מעביר בתוכן את

האינפורמציה

❖ כמה רשומות שאלה וכמה רשומות תשובה קיבלתם

```

Authority RRs: 0
Additional RRs: 0
Queries
  www.google.com: type A, class IN
    Name: www.google.com
    [Name Length: 14]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
Answers

```

נשים לב שיש לנו גם שדה Query ברשומה. פתחו את שדה ה Query. האם אתם מזהים אותו?

הסבר: בכל רשומת תשובה בפרוטוקול ה DNS משלחת גם השאילתה

נסתכל סוף כל סוף בתשובה עצמה:

```

Answers
  www.google.com: type A, class IN, addr 216.58.213.228
    Name: www.google.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 206
    Data length: 4
    Address: www.google.com (216.58.213.228)

```

קיימים שלשת השדות המוכרים לנו כבר:

- Name – שם ה domain שאת ה ip שלו אנחנו מחפשים
- Type – סוג השאילתה (לדוגמא A או PTR)
- Class – IN

אליהם נוספו 3 השדות:

- Time to live – כמה זמן לשמור את תוכן הרשומה
- Data Length – 4 בתים. חישבו למה אורך התשובה 4 בתים?
- Address – סוף כל סוף!!!

כתבו במסמך
המענה את ה ip
שקיבלתם והסבירו
למה אורך
התשובה 4 בתים



עבודה מהנה