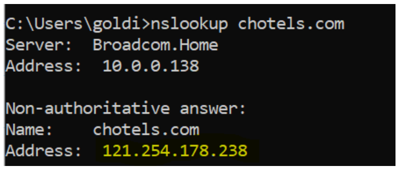
בס"ד

תקשורת ומחשוב – מטלה 2

מגישים: חיים גולדפישר 315599563, אור יצחק 208936039

שאלה 1:

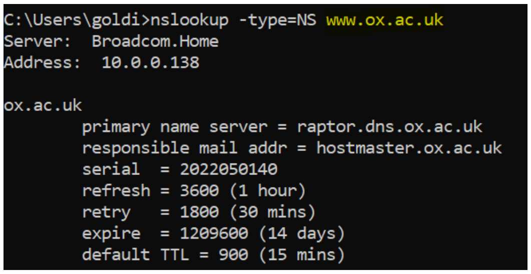
הכתובת היא 121.254.178.238.



```
C:\Users\goldi>nslookup chotels.com
Server:  Broadcom.Home
Address:  10.0.0.138

Non-authoritative answer:
Name:    chotels.com
Address:  121.254.178.238
```

שאלה 2:

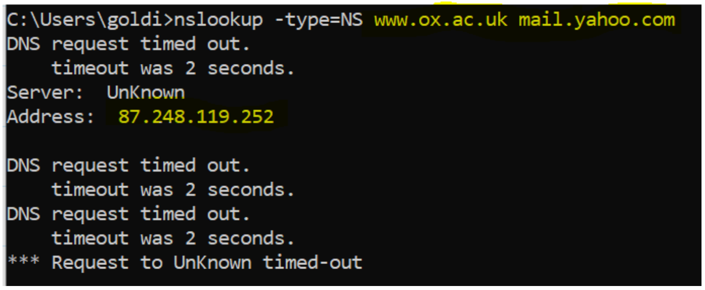
raptor.dns.ox.ac.uk, hostmaster.ox.ac.uk עבור אוניברסיטת אוקספורד שבאנגליה:



```
C:\Users\goldi>nslookup -type=NS www.ox.ac.uk
Server:  Broadcom.Home
Address:  10.0.0.138

ox.ac.uk
        primary name server = raptor.dns.ox.ac.uk
        responsible mail addr = hostmaster.ox.ac.uk
        serial  = 2022050140
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 900 (15 mins)
```

שאלה 3:

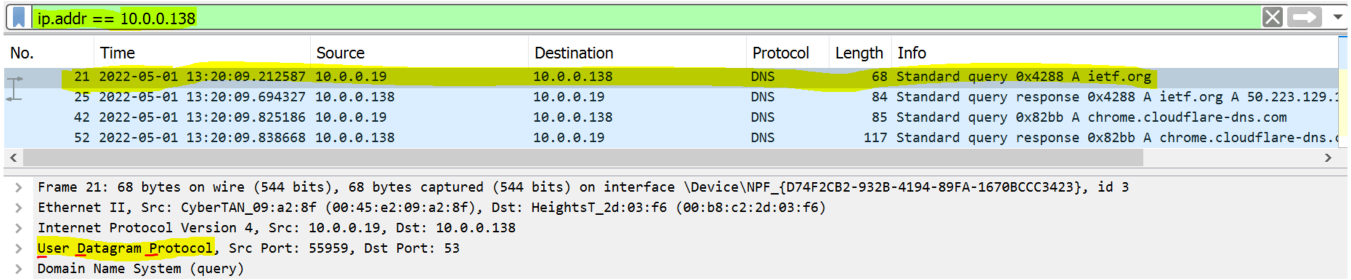
הכתובת היא 87.248.119.252.



```
C:\Users\goldi>nslookup -type=NS www.ox.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.119.252

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

שאלה 4:

UDP – User Datagram Protocol.



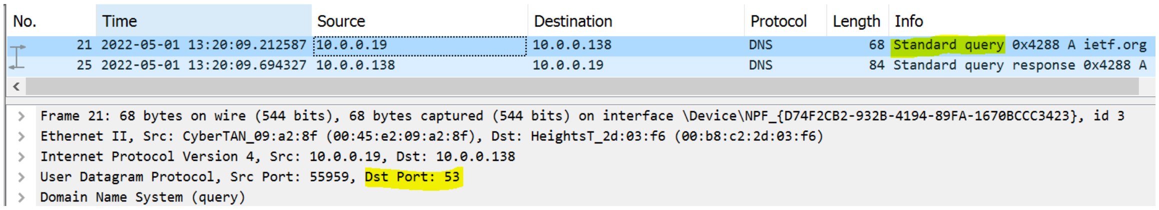
ip.addr == 10.0.0.138

No.	Time	Source	Destination	Protocol	Length	Info
21	2022-05-01 13:20:09.212587	10.0.0.19	10.0.0.138	DNS	68	Standard query 0x4288 A ietf.org
25	2022-05-01 13:20:09.694327	10.0.0.138	10.0.0.19	DNS	84	Standard query response 0x4288 A ietf.org A 50.223.129.1
42	2022-05-01 13:20:09.825186	10.0.0.19	10.0.0.138	DNS	85	Standard query 0x82bb A chrome.cloudflare-dns.com
52	2022-05-01 13:20:09.838668	10.0.0.138	10.0.0.19	DNS	117	Standard query response 0x82bb A chrome.cloudflare-dns.c

```
> Frame 21: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 55959, Dst Port: 53
> Domain Name System (query)
```

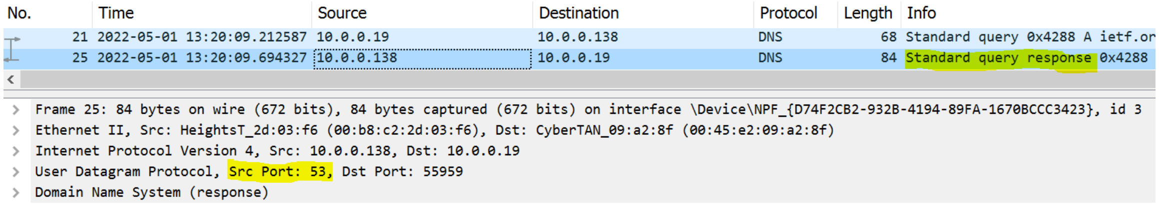
שאלה 5:

היעד של השאילתה הוא פורט 53:



```
No.     Time                        Source              Destination         Protocol  Length  Info
     21 2022-05-01 13:20:09.212587  10.0.0.19           10.0.0.138          DNS           68  Standard query 0x4288 A ietf.org
     25 2022-05-01 13:20:09.694327  10.0.0.138          10.0.0.19           DNS           84  Standard query response 0x4288 A

> Frame 21: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 55959, Dst Port: 53
> Domain Name System (query)
```

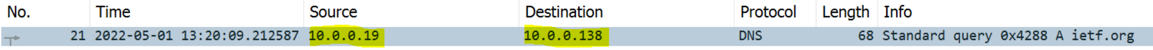
המקור של התגובה לשאילתה הוא גם כן פורט 53:



```
No.     Time                        Source              Destination         Protocol  Length  Info
     21 2022-05-01 13:20:09.212587  10.0.0.19           10.0.0.138          DNS           68  Standard query 0x4288 A ietf.or
     25 2022-05-01 13:20:09.694327  10.0.0.138          10.0.0.19           DNS           84  Standard query response 0x4288

> Frame 25: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.19
> User Datagram Protocol, Src Port: 53, Dst Port: 55959
> Domain Name System (response)
```

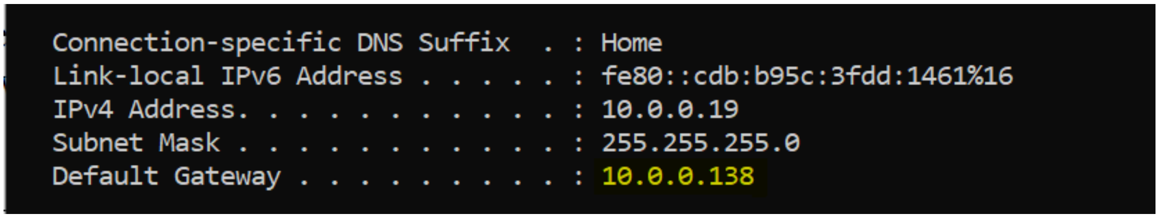
שאלה 6:

המקור: 10.0.0.19. היעד: 10.0.0.138.



```
No.     Time                        Source              Destination         Protocol  Length  Info
     21 2022-05-01 13:20:09.212587  10.0.0.19           10.0.0.138          DNS           68  Standard query 0x4288 A ietf.org
```

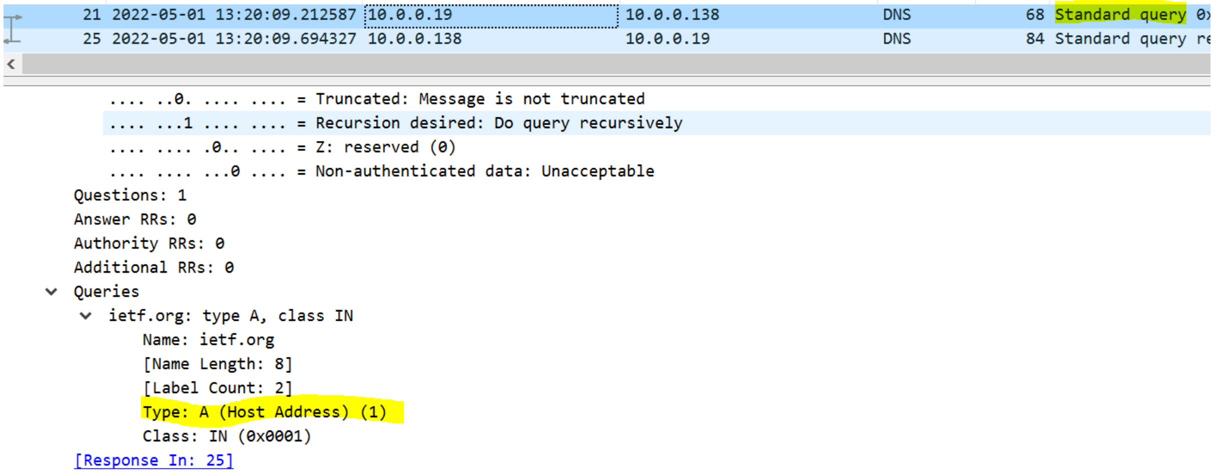
מהרצת הפקודה נראה שהכתובת זהה:



```
   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::cdb:b95c:3fdd:1461%16
   IPv4 Address. . . . . . . . . . . : 10.0.0.19
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.138
```

שאלה 7:

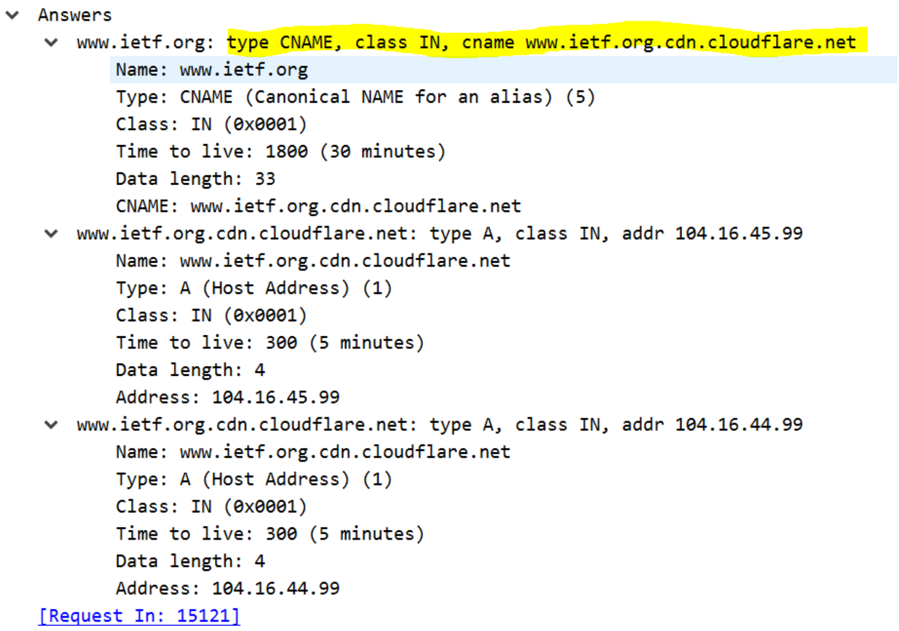
נראה שהשאילתה אינה מכילה תשובה כלשהי. סוג השאילתה הוא A – Host Address.



```
     21 2022-05-01 13:20:09.212587  10.0.0.19           10.0.0.138          DNS           68  Standard query 0x
     25 2022-05-01 13:20:09.694327  10.0.0.138          10.0.0.19           DNS           84  Standard query re

          .... ..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
    v Queries
      v ietf.org: type A, class IN
            Name: ietf.org
            [Name Length: 8]
            [Label Count: 2]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
      [Response In: 25]
```

שאלה 8:

ניכר שיש לנו בסה"כ 3 תשובות, נציג אותן:

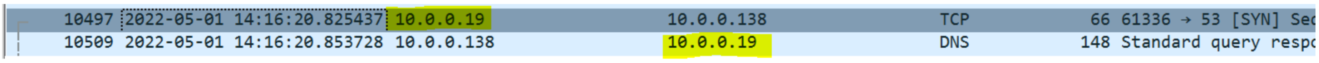


```
v Answers
  v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
[Request In: 15121]
```

מה הן מכילות: שם – כתובת אתר, סוג, כתובת איי פי, זמן שנותר לו "לחיות", מחלקה ואורך הדאטה.

שאלה 9:

כן. בשניהם 10.0.0.19.



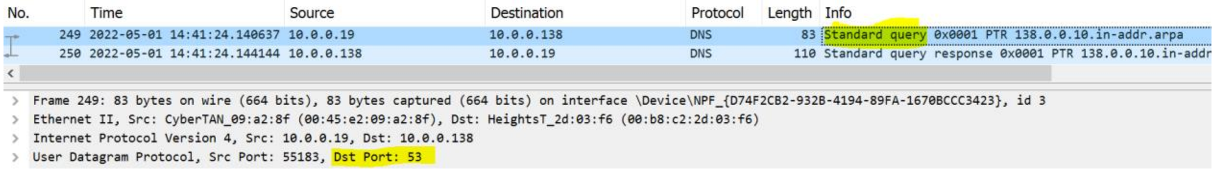
```
10497 2022-05-01 14:16:20.825437 10.0.0.19         10.0.0.138        TCP        66 61336 → 53 [SYN] Sec
10509 2022-05-01 14:16:20.853728 10.0.0.138        10.0.0.19         DNS       148 Standard query respc
```

שאלה 10:

אני לא מוצא ברשימת החבילות שאילתות כאלה, אז כנראה שאין.

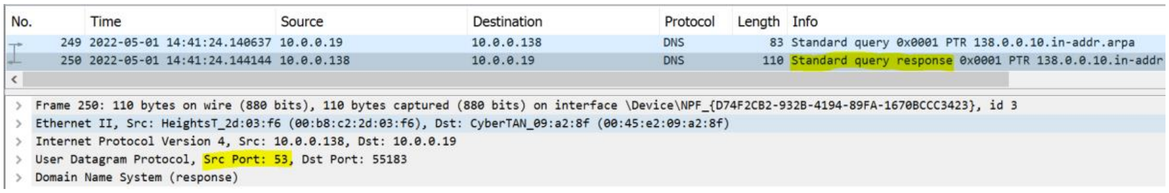
שאלה 11:

בשאילתה, פורט ה**יעד** הוא 53:



```
No.   Time                       Source       Destination   Protocol  Length  Info
  249 2022-05-01 14:41:24.140637 10.0.0.19    10.0.0.138    DNS           83  Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
  250 2022-05-01 14:41:24.144144 10.0.0.138   10.0.0.19     DNS          110  Standard query response 0x0001 PTR 138.0.0.10.in-addr

> Frame 249: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 55183, Dst Port: 53
```

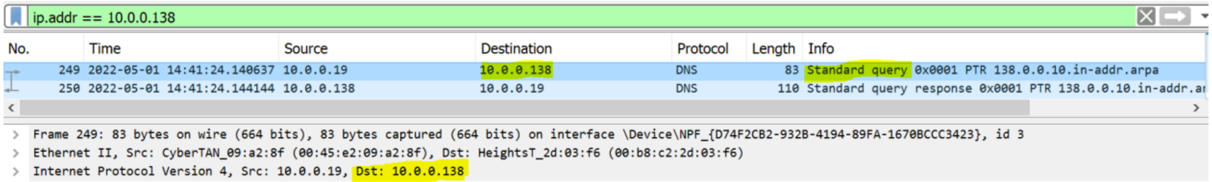
בתגובה לשאילתה, פורט ה**מקור** הוא גם 53:



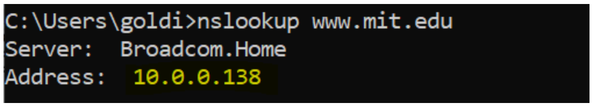
```
No.   Time                       Source       Destination   Protocol  Length  Info
  249 2022-05-01 14:41:24.140637 10.0.0.19    10.0.0.138    DNS           83  Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
  250 2022-05-01 14:41:24.144144 10.0.0.138   10.0.0.19     DNS          110  Standard query response 0x0001 PTR 138.0.0.10.in-addr

> Frame 250: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.19
> User Datagram Protocol, Src Port: 53, Dst Port: 55183
> Domain Name System (response)
```

שאלה 12:

נשלח אל הכתובת 10.0.0.138, כתובת האייפי של המחשב שלי. ניתן לראות זאת גם בפקודה שעשיתי.



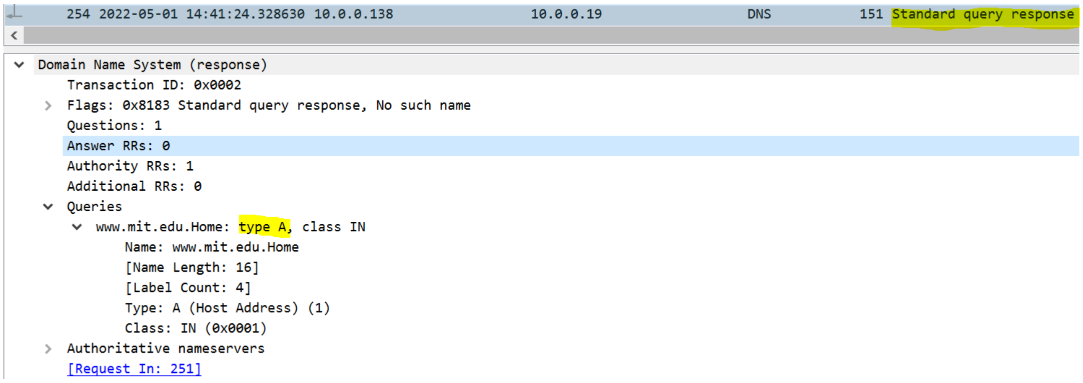
```
ip.addr == 10.0.0.138

No.  Time                        Source      Destination  Protocol  Length  Info
249  2022-05-01 14:41:24.140637  10.0.0.19   10.0.0.138   DNS           83  Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
250  2022-05-01 14:41:24.144144  10.0.0.138  10.0.0.19    DNS          110  Standard query response 0x0001 PTR 138.0.0.10.in-addr.ar

> Frame 249: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
```



```
C:\Users\goldi>nslookup www.mit.edu
Server:   Broadcom.Home
Address:  10.0.0.138
```

שאלה 13:

בדיוק כמו בשאלה 7, השאילתה אינה מכילה תשובה כלשהי, וסוג השאילתה הוא A.

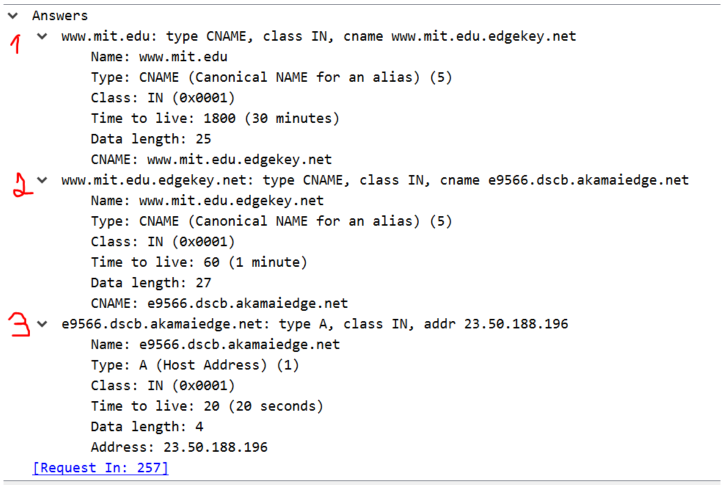


```
254 2022-05-01 14:41:24.328630 10.0.0.138          10.0.0.19          DNS          151 Standard query response

v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v www.mit.edu.Home: type A, class IN
        Name: www.mit.edu.Home
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Authoritative nameservers
    [Request In: 251]
```

שאלה 14:

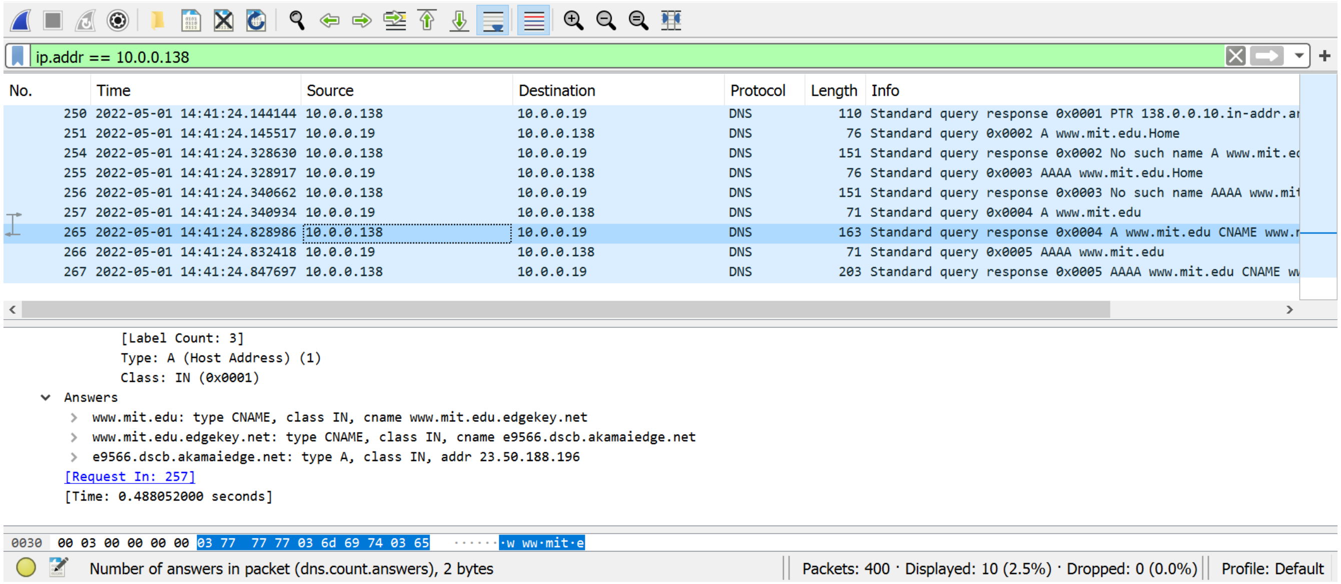
3 תשובות, מכילות:

Name, Type, Class, Time to live, Data length, CName.



```
v Answers
1 v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: www.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
2 v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        Name: www.mit.edu.edgekey.net
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 27
        CNAME: e9566.dscb.akamaiedge.net
3 v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.50.188.196
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 23.50.188.196
  [Request In: 257]
```

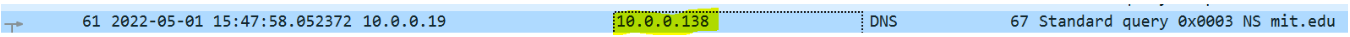
שאלה 15: מצורף צילום מסך של הווירשארק -



```
ip.addr == 10.0.0.138

No.  Time                        Source       Destination  Protocol Length Info
 250 2022-05-01 14:41:24.144144 10.0.0.138   10.0.0.19    DNS         110 Standard query response 0x0001 PTR 138.0.0.10.in-addr.ar
 251 2022-05-01 14:41:24.145517 10.0.0.19    10.0.0.138   DNS          76 Standard query 0x0002 A www.mit.edu.Home
 254 2022-05-01 14:41:24.328630 10.0.0.138   10.0.0.19    DNS         151 Standard query response 0x0002 No such name A www.mit.ec
 255 2022-05-01 14:41:24.328917 10.0.0.19    10.0.0.138   DNS          76 Standard query 0x0003 AAAA www.mit.edu.Home
 256 2022-05-01 14:41:24.340662 10.0.0.138   10.0.0.19    DNS         151 Standard query response 0x0003 No such name AAAA www.mit
 257 2022-05-01 14:41:24.340934 10.0.0.19    10.0.0.138   DNS          71 Standard query 0x0004 A www.mit.edu
 265 2022-05-01 14:41:24.828986 10.0.0.138   10.0.0.19    DNS         163 Standard query response 0x0004 A www.mit.edu CNAME www.r
 266 2022-05-01 14:41:24.832418 10.0.0.19    10.0.0.138   DNS          71 Standard query 0x0005 AAAA www.mit.edu
 267 2022-05-01 14:41:24.847697 10.0.0.138   10.0.0.19    DNS         203 Standard query response 0x0005 AAAA www.mit.edu CNAME wv

            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers
        > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.50.188.196
    [Request In: 257]
    [Time: 0.488052000 seconds]

0030  00 03 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ······w ww·mit·e

Number of answers in packet (dns.count.answers), 2 bytes   Packets: 400 · Displayed: 10 (2.5%) · Dropped: 0 (0.0%)   Profile: Default
```

שאלה 16:

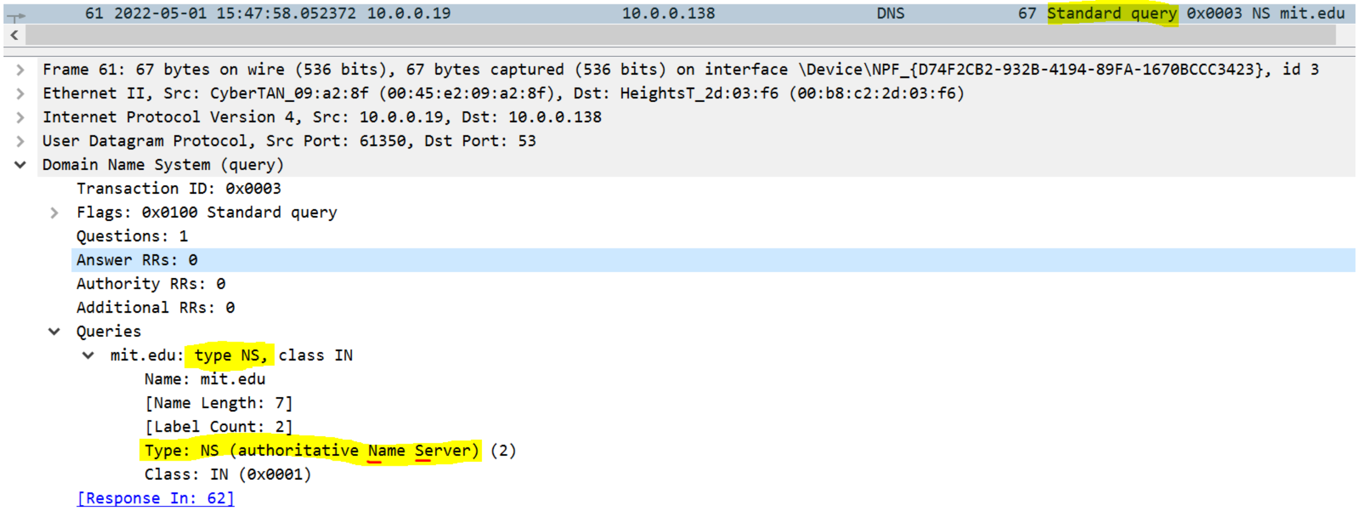
השאילתה נשלחה אל הכתובת 10.0.0.138. כן, זו הכתובת של שרת ה'די אן אס' בברירת המחדל שלי.



```
  61 2022-05-01 15:47:58.052372 10.0.0.19          10.0.0.138          DNS        67 Standard query 0x0003 NS mit.edu
```

שאלה 17:

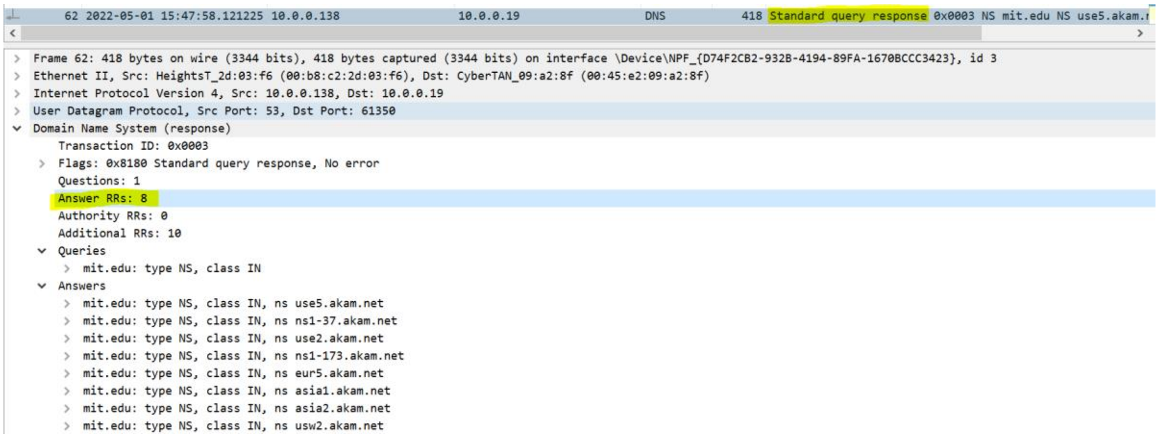
השאילתה אינה מכילה תשובה. סוג השאילתה הוא NS – authoritative Name Server



```
  61 2022-05-01 15:47:58.052372 10.0.0.19          10.0.0.138          DNS        67 Standard query 0x0003 NS mit.edu

> Frame 61: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 61350, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x0003
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   v Queries
      v mit.edu: type NS, class IN
           Name: mit.edu
           [Name Length: 7]
           [Label Count: 2]
           Type: NS (authoritative Name Server) (2)
           Class: IN (0x0001)
     [Response In: 62]
```

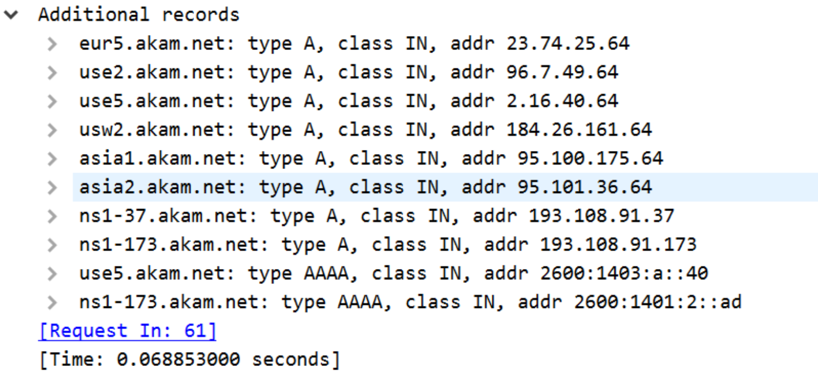
שאלה 18:

התקבלו 8 תשובות. נראה שאין בתשובות כתובות אייפי:



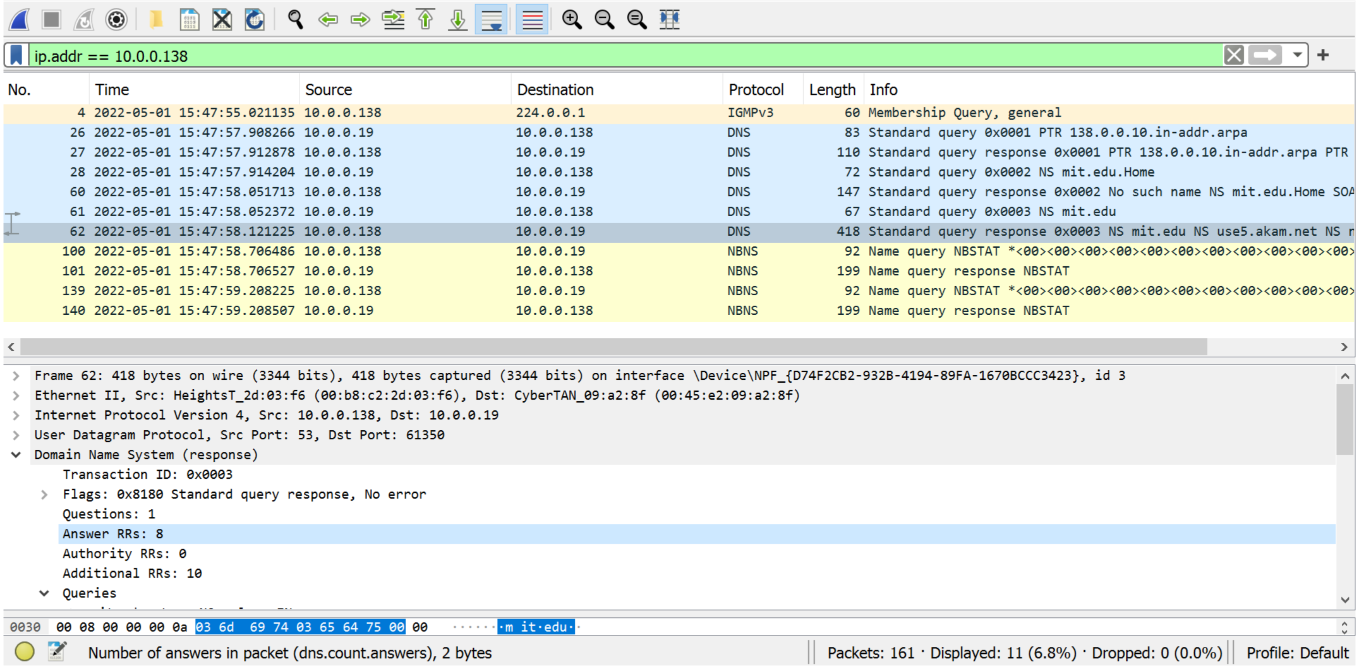
```
62 2022-05-01 15:47:58.121225 10.0.0.138          10.0.0.19          DNS          418 Standard query response 0x0003 NS mit.edu NS use5.akam.r

> Frame 62: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.19
> User Datagram Protocol, Src Port: 53, Dst Port: 61350
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 10
  v Queries
    > mit.edu: type NS, class IN
  v Answers
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
```

אך בהמשך הפרוטוקול, מופיעה רשומה שמכילה את כתובות האייפי בשם Additional records :



```
v Additional records
    > eur5.akam.net: type A, class IN, addr 23.74.25.64
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > use5.akam.net: type A, class IN, addr 2.16.40.64
    > usw2.akam.net: type A, class IN, addr 184.26.161.64
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    > asia2.akam.net: type A, class IN, addr 95.101.36.64
    > ns1-37.akam.net: type A, class IN, addr 193.108.91.37
    > ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    > use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    > ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
  [Request In: 61]
  [Time: 0.068853000 seconds]
```

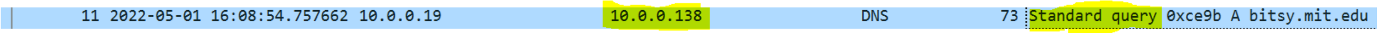
שאלה 19: מצורף צילום מסך של הווירשארק –



```
ip.addr == 10.0.0.138

No.   Time                          Source        Destination   Protocol  Length Info
    4 2022-05-01 15:47:55.021135 10.0.0.138    224.0.0.1     IGMPv3        60 Membership Query, general
   26 2022-05-01 15:47:57.908266 10.0.0.19     10.0.0.138    DNS           83 Standard query 0x0001 PTR 138.0.0.10.in-addr.arpa
   27 2022-05-01 15:47:57.912878 10.0.0.138    10.0.0.19     DNS          110 Standard query response 0x0001 PTR 138.0.0.10.in-addr.arpa PTR
   28 2022-05-01 15:47:57.914204 10.0.0.19     10.0.0.138    DNS           72 Standard query 0x0002 NS mit.edu.Home
   60 2022-05-01 15:47:58.051713 10.0.0.138    10.0.0.19     DNS          147 Standard query response 0x0002 No such name NS mit.edu.Home SOA
   61 2022-05-01 15:47:58.052372 10.0.0.19     10.0.0.138    DNS           67 Standard query 0x0003 NS mit.edu
   62 2022-05-01 15:47:58.121225 10.0.0.138    10.0.0.19     DNS          418 Standard query response 0x0003 NS mit.edu NS use5.akam.net NS r
  100 2022-05-01 15:47:58.706486 10.0.0.138    10.0.0.19     NBNS          92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00>
  101 2022-05-01 15:47:58.706527 10.0.0.19     10.0.0.138    NBNS         199 Name query response NBSTAT
  139 2022-05-01 15:47:59.208225 10.0.0.138    10.0.0.19     NBNS          92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00>
  140 2022-05-01 15:47:59.208507 10.0.0.19     10.0.0.138    NBNS         199 Name query response NBSTAT

> Frame 62: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
> Internet Protocol Version 4, Src: 10.0.0.138, Dst: 10.0.0.19
> User Datagram Protocol, Src Port: 53, Dst Port: 61350
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 10
  v Queries

0030  00 08 00 00 00 0a 03 6d  69 74 03 65 64 75 00 00   ······m it·edu··

Number of answers in packet (dns.count.answers), 2 bytes    Packets: 161 · Displayed: 11 (6.8%) · Dropped: 0 (0.0%)    Profile: Default
```

שאלה 20:

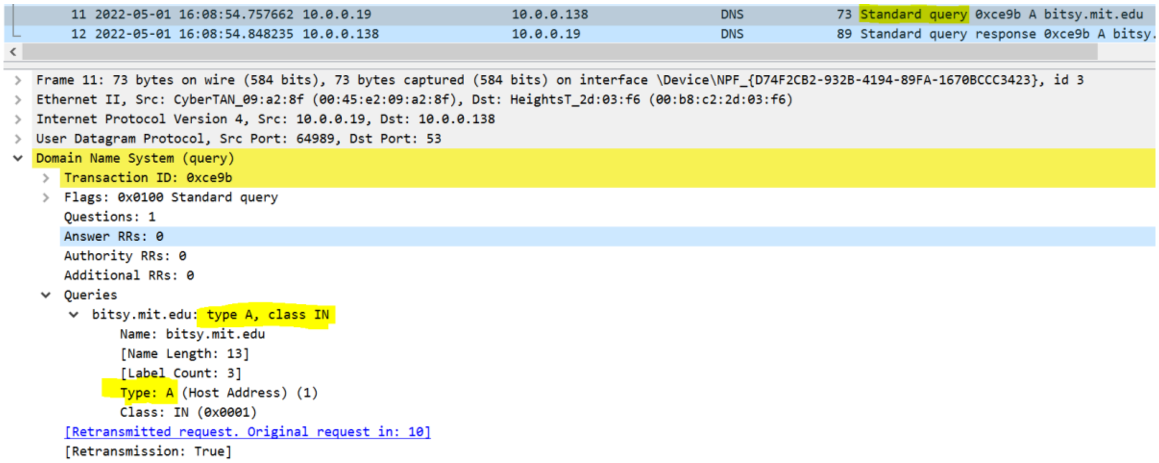
השאילתה נשלחה אל הכתובת 10.0.0.138. כן, זו הכתובת של שרת ה'די אן אס' בברירת המחדל שלי.



```
 11 2022-05-01 16:08:54.757662 10.0.0.19          10.0.0.138          DNS          73 Standard query 0xce9b A bitsy.mit.edu
```

שאלה 21:

השאילתה אינה מכילה תשובה כלשהי, וסוג השאילתה הוא A.

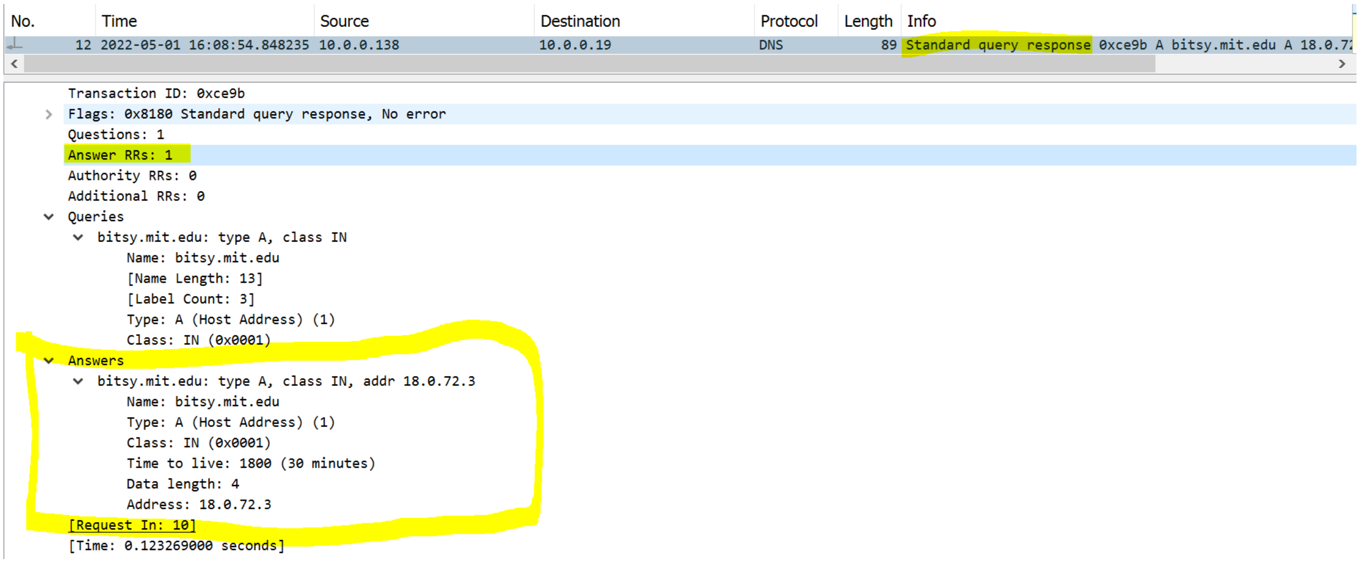


```
 11 2022-05-01 16:08:54.757662 10.0.0.19          10.0.0.138          DNS          73 Standard query 0xce9b A bitsy.mit.edu
 12 2022-05-01 16:08:54.848235 10.0.0.138         10.0.0.19           DNS          89 Standard query response 0xce9b A bitsy.

> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 64989, Dst Port: 53
v Domain Name System (query)
    > Transaction ID: 0xce9b
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    v Queries
        v bitsy.mit.edu: type A, class IN
              Name: bitsy.mit.edu
              [Name Length: 13]
              [Label Count: 3]
              Type: A (Host Address) (1)
              Class: IN (0x0001)
      [Retransmitted request. Original request in: 10]
      [Retransmission: True]
```

שאלה 22:

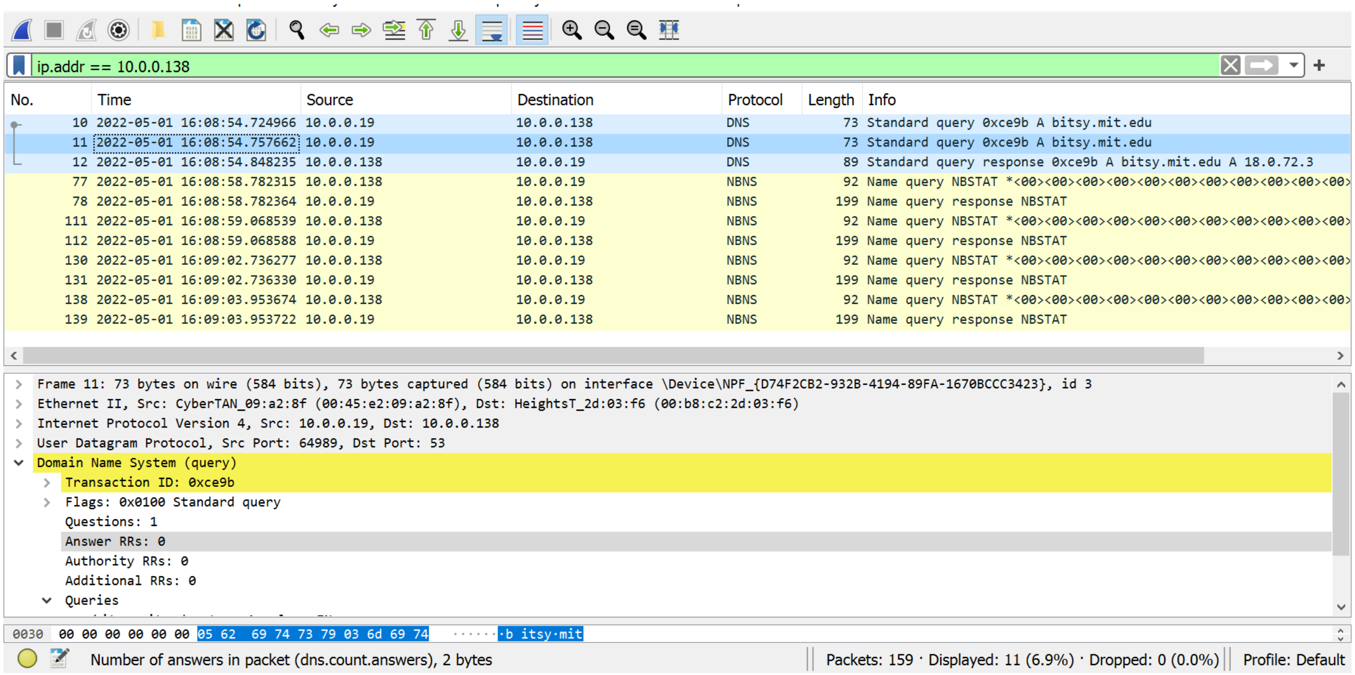
תשובה אחת. מכילה:

Name, Type, Class, Time to live, Data length, Address.



```
No.      Time                        Source           Destination        Protocol  Length Info
   12 2022-05-01 16:08:54.848235 10.0.0.138       10.0.0.19          DNS           89 Standard query response 0xce9b A bitsy.mit.edu A 18.0.7

        Transaction ID: 0xce9b
      > Flags: 0x8180 Standard query response, No error
        Questions: 1
        Answer RRs: 1
        Authority RRs: 0
        Additional RRs: 0
      v Queries
          v bitsy.mit.edu: type A, class IN
                Name: bitsy.mit.edu
                [Name Length: 13]
                [Label Count: 3]
                Type: A (Host Address) (1)
                Class: IN (0x0001)
      v Answers
          v bitsy.mit.edu: type A, class IN, addr 18.0.72.3
                Name: bitsy.mit.edu
                Type: A (Host Address) (1)
                Class: IN (0x0001)
                Time to live: 1800 (30 minutes)
                Data length: 4
                Address: 18.0.72.3
        [Request In: 10]
        [Time: 0.123269000 seconds]
```

שאלה 23: מצורף צילום מסך של הווירשארק –



ip.addr == 10.0.0.138

```
No.   Time                        Source       Destination   Protocol  Length  Info
   10 2022-05-01 16:08:54.724966 10.0.0.19    10.0.0.138    DNS         73 Standard query 0xce9b A bitsy.mit.edu
   11 2022-05-01 16:08:54.757662 10.0.0.19    10.0.0.138    DNS         73 Standard query 0xce9b A bitsy.mit.edu
   12 2022-05-01 16:08:54.848235 10.0.0.138   10.0.0.19     DNS         89 Standard query response 0xce9b A bitsy.mit.edu A 18.0.72.3
   77 2022-05-01 16:08:58.782315 10.0.0.138   10.0.0.19     NBNS        92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00>
   78 2022-05-01 16:08:58.782364 10.0.0.19    10.0.0.138    NBNS       199 Name query response NBSTAT
  111 2022-05-01 16:08:59.068539 10.0.0.138   10.0.0.19     NBNS        92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00>
  112 2022-05-01 16:08:59.068588 10.0.0.19    10.0.0.138    NBNS       199 Name query response NBSTAT
  130 2022-05-01 16:09:02.736277 10.0.0.138   10.0.0.19     NBNS        92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00>
  131 2022-05-01 16:09:02.736330 10.0.0.19    10.0.0.138    NBNS       199 Name query response NBSTAT
  138 2022-05-01 16:09:03.953674 10.0.0.138   10.0.0.19     NBNS        92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00>
  139 2022-05-01 16:09:03.953722 10.0.0.19    10.0.0.138    NBNS       199 Name query response NBSTAT
```

```
> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
> Internet Protocol Version 4, Src: 10.0.0.19, Dst: 10.0.0.138
> User Datagram Protocol, Src Port: 64989, Dst Port: 53
v Domain Name System (query)
    > Transaction ID: 0xce9b
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    v Queries
```

```
0030  00 00 00 00 00 00 05 62  69 74 73 79 03 6d 69 74   ······b itsy·mit
```

Number of answers in packet (dns.count.answers), 2 bytes

Packets: 159 · Displayed: 11 (6.9%) · Dropped: 0 (0.0%)

Profile: Default