Astrid Delestine

1/13/2023

ECE_372

Prof. Bechir Hamdaoui

Overview:

This lab is designed to introduce the concepts of the nslookup tool and the ipconfig tool to see certain sets of data. Additionally This lab teaches the student how to trace DNS packets using Wireshark.

Content:

Firstly the student focus on the nslookup tool and how it works. The student then uses the tool to query www.mit.edu essentially asking for the IP address of www.mit.edu. The student then adds the -type flag setting it to NS causing the nslookup tool to find a NS type record to the local DNS server. Then the student runs the nslookup tool with two different website URLs the second one being the DNS server to query for the address of the second.

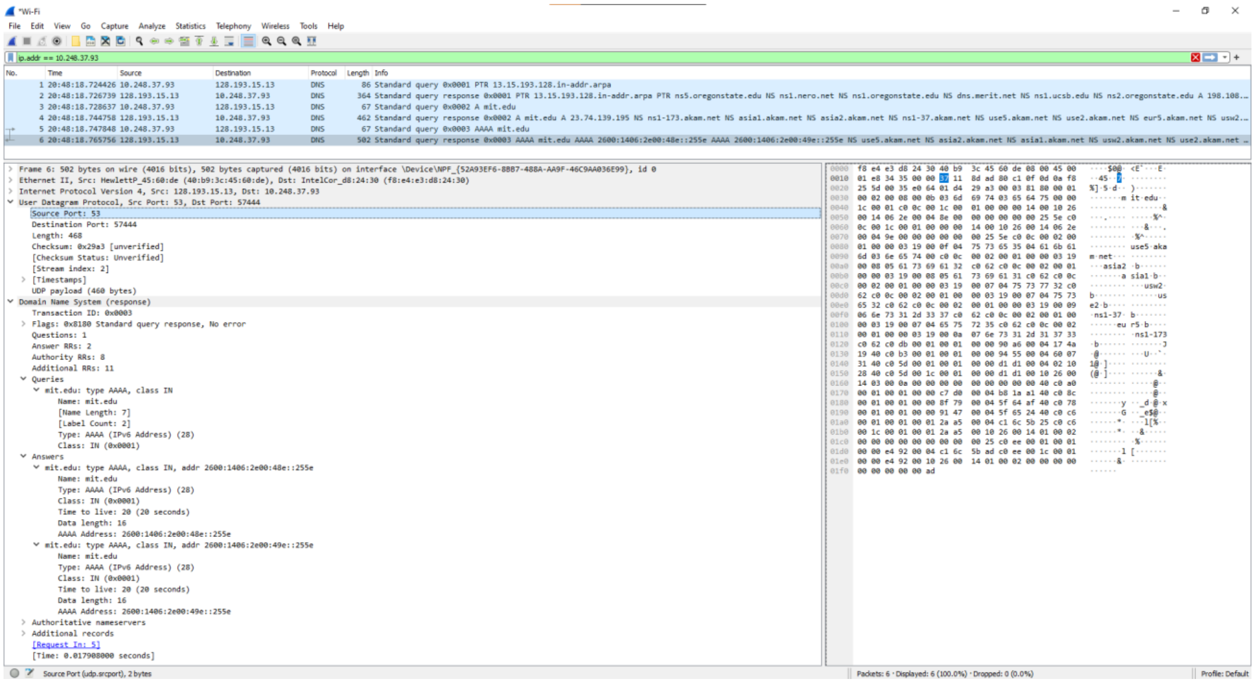
Secondly the student moves to the ipconfig tool and learns exactly what it does, and how it can help display information. The student then moves to tracing DNS with Wireshark and is allowed to experiment with searching through Wireshark for DNS signals. Then they are introduced to the questions which can be seen below, essentially teaching the student what to look for when doing DNS tracing.

Requested Questions/Information:

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
   a. Ran nslookup to find the address of baidu.com a search engine like google, but for China. The found IP addresses were 39.156.66.10 and 110.242.68.66
2. Run nslookup to determine the authoritative DNS servers for a university in Europe
   a. Ran nslookup to find the authoritative DNS for the University of Munich. The found DNS servers addresses were:
      dns1.lrz.de : 129.187.19.183
      dns2.lrz.Bayern : 141.40.9.211
      dns3.lrz.eu : 78.128.211.180
3. Run nslookup so that one of the DNS servers obtained in Question b is queried for the mail servers for Yahoo! Mail. What is its IP address?
   a. Using the first DNS server obtained in Q1B The college was unable to find www.yahoo.com or www.mail.yahoo.com. For this reason, I tested the same lookup command however I used googles DNS server, and received 98.137.11.164 and 98.137.11.163
4. Locate the DNS query and response messages. Were they sent over TCP or UDP
   a. It was hard to tell, however I believe that it was UDP, I did end up finding it after a bit. [1]

5. What is the destination port for the DNS query message? What is the source port of DNS query message.
    a. The source port was 49335 and the destination port was 53.
6. To what IP address is the DNS query message sent? Use Ipconfig to determine the IP address of your local DNS server. Are the two IP addresses the same?
    a. The DNS query was sent to 128.193.15.23, ipconfig says the local DNS servers are 128.193.15.13 and 128.193.15.12. Clearly these IP addresses are not the same.
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any answers?
    a. The query message does not contain any answers, As for the type, it is a standard query, or it is a IPV4 query.
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
    a. Contains 3 answers, The first one contains the name of the website, its type (CNAME) its ttl and data length and its class. The second and third one both have the same labes however the name is different, and the class is IN.
9. Examine the subsequent TCP SYN package sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response?
    a. Yes, under ipv4hint, on the DNS answers it lists the addresses. The first address is the same.
10. This webpage contains images. Before retrieving each image, does your host issue new DNS requests?
    a. Not as far as I can tell. It does issue one more, but not one for each image.
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    a. Destination port is 53 and source port is 57444
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    a. The DNS query message was sent to my default DNS server, This address was 128.193.15.13
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    a. The type of the query is AAAA, no answers are in the query.
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
    a. The response message has 2 answers, and each of them contains a name, type, class, ttl, data length, and AAAA address.
15. Provide a screenshot
    a. See [S1]
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    a. The address query was made to my local dns server, being 128.193.15.13

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    a. The query message had type of NS and contained no answers.
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
    a. The MIT nameservers that are given can be seen in [S2], and the IP addresses are not given inside of the answers, however they are given under additional records [S3]
19. Provide a screenshot.
    a. Seen as [S4]
20. To what IP address is the DNS query message sent? Is this the IP address of you default local DNS server? If not, what does the IP address correspond to? (8.8.8.8)
    a. It is sent to the 8.8.8.8 server (googles dns server) This corresponds to the server that was inputted as the second parameter for the nslookup command.
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? (8.8.8.8)
    a. They type of this DNS query is AAAA, there are no answers in the query.
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain? (8.8.8.8)
    a. As I was flipping through the different DNS requests I found that only the first request resulted in an answer. Which was a pointer from google 8.8.8.8 [S5] The last query response did return an authoritative nameserver [S6].
23. Provide a screenshot. (8.8.8.8)
    a. Seen as [S7]


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.248.37.93

```
No.  Time             Source          Destination     Protocol Length Info
   1 20:48:18.724426 10.248.37.93    128.193.15.13   DNS        86 Standard query 0x0001 PTR 13.15.193.128.in-addr.arpa
   2 20:48:18.726739 128.193.15.13   10.248.37.93    DNS       364 Standard query response 0x0001 PTR 13.15.193.128.in-addr.arpa PTR ns5.oregonstate.edu NS ns1.nero.net NS ns1.oregonstate.edu NS dns.merit.net NS ns1.ucsb.edu NS ns2.oregonstate.edu A 198.108.…
   3 20:48:18.728637 10.248.37.93    128.193.15.13   DNS        67 Standard query 0x0002 A mit.edu
   4 20:48:18.744758 128.193.15.13   10.248.37.93    DNS       462 Standard query response 0x0002 A mit.edu A 23.74.139.195 NS ns1-173.akam.net NS asia1.akam.net NS asia2.akam.net NS ns1-37.akam.net NS use5.akam.net NS use2.akam.net NS eur5.akam.net NS usw2.…
   5 20:48:18.747848 10.248.37.93    128.193.15.13   DNS        67 Standard query 0x0003 AAAA mit.edu
   6 20:48:18.765756 128.193.15.13   10.248.37.93    DNS       502 Standard query response 0x0003 AAAA mit.edu AAAA 2600:1406:2e00:48e::255e AAAA 2600:1406:2e00:49e::255e NS use5.akam.net NS asia2.akam.net NS asia1.akam.net NS usw2.akam.net NS use2.akam.net …
```

```
> Frame 6: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface \Device\NPF_{52A93EF6-8BB7-488A-AA9F-46C9AA036E99}, id 0
> Ethernet II, Src: HewlettP_45:60:de (40:b9:3c:45:60:de), Dst: IntelCor_d8:24:30 (f8:e4:e3:d8:24:30)
> Internet Protocol Version 4, Src: 128.193.15.13, Dst: 10.248.37.93
v User Datagram Protocol, Src Port: 53, Dst Port: 57444
    Source Port: 53
    Destination Port: 57444
    Length: 468
    Checksum: 0x29a3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (460 bytes)
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 8
    Additional RRs: 11
  v Queries
    v mit.edu: type AAAA, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  v Answers
    v mit.edu: type AAAA, class IN, addr 2600:1406:2e00:48e::255e
        Name: mit.edu
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 16
        AAAA Address: 2600:1406:2e00:48e::255e
    v mit.edu: type AAAA, class IN, addr 2600:1406:2e00:49e::255e
        Name: mit.edu
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 16
        AAAA Address: 2600:1406:2e00:49e::255e
  > Authoritative nameservers
  > Additional records
    [Request In: 5]
    [Time: 0.017908000 seconds]
```

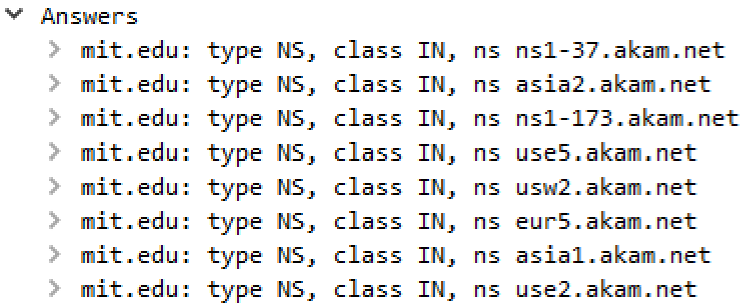
```
0000  f8 e4 e3 d8 24 30 40 b9  3c 45 60 de 08 00 45 00   ····$0@· <E`···E·
0010  01 e8 34 35 00 00 37 11  8d ad 80 c1 0f 0d 0a f8   ··45··7· ········
0020  25 5d 00 35 e0 64 01 d4  29 a3 00 03 81 80 00 01   %]·5·d·· )·······
0030  00 02 00 08 00 0b 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  1c 00 01 c0 0c 00 1c 00  01 00 00 00 14 00 10 26   ········ ·······&
0050  00 14 06 2e 00 04 8e 00  00 00 00 00 00 25 5e c0   ···.···· ·····%^·
0060  0c 00 1c 00 01 00 00 00  14 00 10 26 00 14 06 2e   ········ ···&···.
0070  00 04 9e 00 00 00 00 00  00 25 5e c0 0c 00 02 00   ········ ·%^·····
0080  01 00 00 03 19 00 0f 04  75 73 65 35 04 61 6b 61   ········ use5·aka
0090  6d 03 6e 65 74 00 c0 0c  00 02 00 01 00 00 03 19   m·net··· ········
00a0  00 08 05 61 73 69 61 32  c0 62 c0 0c 00 02 00 01   ···asia2 ·b······
00b0  00 00 03 19 00 08 05 61  73 69 61 31 c0 62 c0 0c   ·······a sia1·b··
00c0  00 02 00 01 00 00 03 19  00 07 04 75 73 77 32 c0   ········ ···usw2·
00d0  62 c0 0c 00 02 00 01 00  00 03 19 00 07 04 75 73   b······· ······us
00e0  65 32 c0 62 c0 0c 00 02  00 01 00 00 03 19 00 09   e2·b···· ········
00f0  06 6e 73 31 2d 33 37 c0  62 c0 0c 00 02 00 01 00   ·ns1-37· b·······
0100  00 03 19 00 07 04 65 75  72 35 c0 62 c0 0c 00 02   ······eu r5·b····
0110  00 01 00 00 03 19 00 0a  07 6e 73 31 2d 31 37 33   ········ ·ns1-173
0120  c0 62 c0 db 00 01 00 01  00 00 90 a6 00 04 17 4a   ·b······ ·······J
0130  19 40 c0 b3 00 01 00 01  00 00 94 55 00 04 60 07   ·@······ ···U··`·
0140  31 40 c0 5d 00 01 00 01  00 00 d1 d1 00 04 02 10   1@·]···· ········
0150  28 40 c0 5d 00 1c 00 01  00 00 d1 d1 00 10 26 00   (@·]···· ······&·
0160  14 03 00 0a 00 00 00 00  00 00 00 00 00 40 c0 a0   ········ ·····@··
0170  00 01 00 01 00 00 c7 d0  00 04 b8 1a a1 40 c0 8c   ········ ·····@··
0180  00 01 00 01 00 00 8f 79  00 04 5f 64 af 40 c0 78   ·······y ··_d·@·x
0190  00 01 00 01 00 00 91 47  00 04 5f 65 24 40 c0 c6   ·······G ··_e$@··
01a0  00 01 00 01 00 01 2a a5  00 04 c1 6c 5b 25 c0 c6   ······*· ···l[%··
01b0  00 1c 00 01 00 01 2a a5  00 10 26 00 14 01 00 02   ······*· ··&·····
01c0  00 00 00 00 00 00 00 00  00 25 c0 ee 00 01 00 01   ········ ·%······
01d0  00 00 e4 92 00 04 c1 6c  5b ad c0 ee 00 1c 00 01   ·······l [·······
01e0  00 00 e4 92 00 10 26 00  14 01 00 02 00 00 00 00   ······&· ········
01f0  00 00 00 00 00 ad                                  ······
```

Source Port (udp.srcport), 2 bytes

Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%)

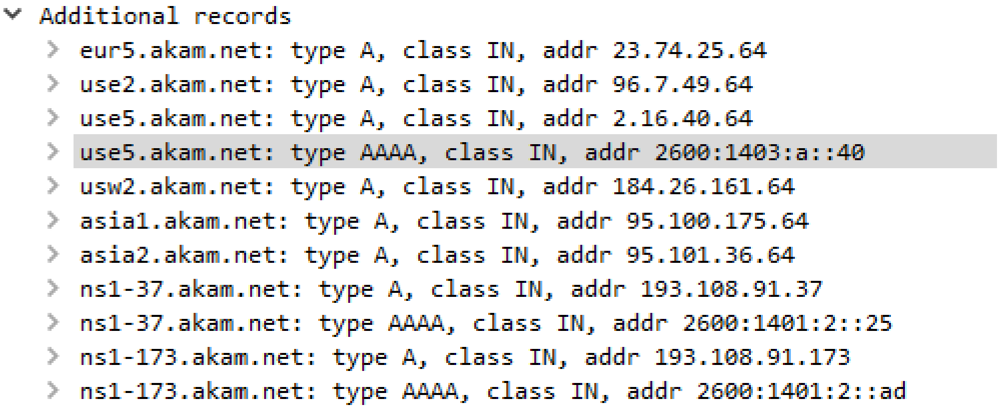
Profile: Default

Figure 1 [S1]



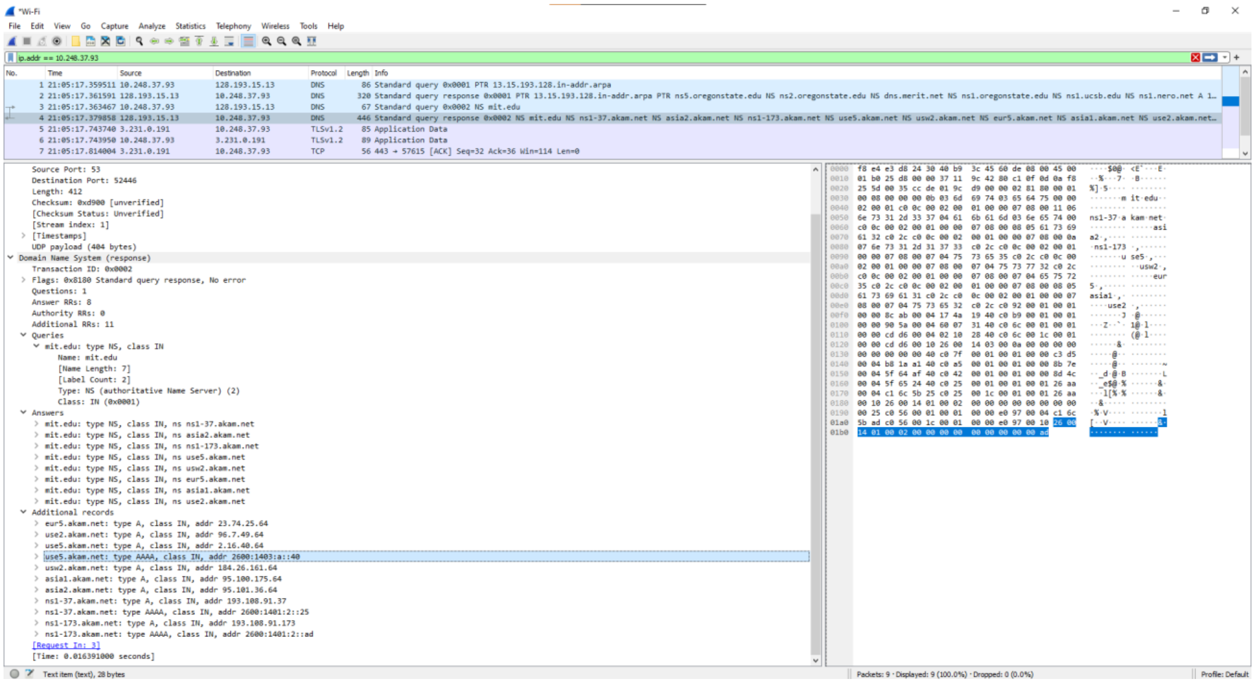
```
⌄ Answers
    › mit.edu: type NS, class IN, ns ns1-37.akam.net
    › mit.edu: type NS, class IN, ns asia2.akam.net
    › mit.edu: type NS, class IN, ns ns1-173.akam.net
    › mit.edu: type NS, class IN, ns use5.akam.net
    › mit.edu: type NS, class IN, ns usw2.akam.net
    › mit.edu: type NS, class IN, ns eur5.akam.net
    › mit.edu: type NS, class IN, ns asia1.akam.net
    › mit.edu: type NS, class IN, ns use2.akam.net
```

Figure 2 [S2]



```
⌄ 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
    › use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    › 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
    › ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
    › ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    › ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
```

Figure 3 [S3]



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.248.37.93

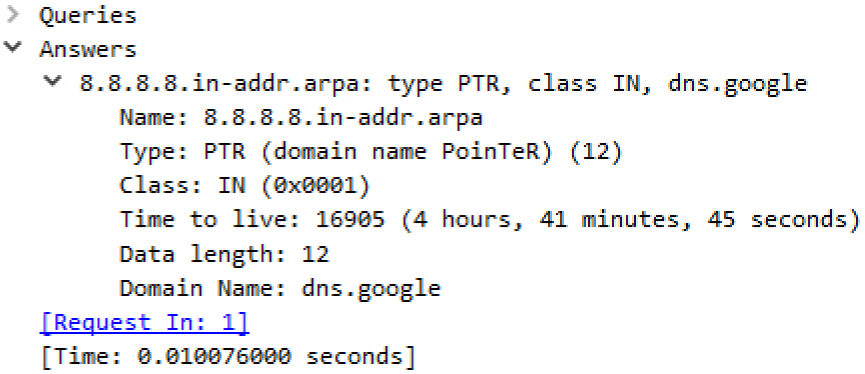
```
No.   Time            Source          Destination     Protocol Length Info
    1 21:05:17.359511 10.248.37.93    128.193.15.13   DNS          86 Standard query 0x0001 PTR 13.15.193.128.in-addr.arpa
    2 21:05:17.361591 128.193.15.13   10.248.37.93    DNS         320 Standard query response 0x0001 PTR 13.15.193.128.in-addr.arpa PTR ns5.oregonstate.edu NS ns2.oregonstate.edu NS dns.merit.net NS ns1.oregonstate.edu NS ns1.ucsb.edu NS ns1.nero.net A 1…
    3 21:05:17.363467 10.248.37.93    128.193.15.13   DNS          67 Standard query 0x0002 NS mit.edu
    4 21:05:17.379858 128.193.15.13   10.248.37.93    DNS         446 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia2.akam.net NS ns1-173.akam.net NS use5.akam.net NS usw2.akam.net NS eur5.akam.net NS asia1.akam.net NS use2.akam.net…
    5 21:05:17.743740 3.231.0.191     10.248.37.93    TLSv1.2      85 Application Data
    6 21:05:17.743950 10.248.37.93    3.231.0.191     TLSv1.2      89 Application Data
    7 21:05:17.814004 3.231.0.191     10.248.37.93    TCP          56 443 → 57615 [ACK] Seq=32 Ack=36 Win=114 Len=0
```

```
    Source Port: 53
    Destination Port: 52446
    Length: 412
    Checksum: 0xd900 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  › [Timestamps]
    UDP payload (404 bytes)
⌄ Domain Name System (response)
    Transaction ID: 0x0002
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 11
  ⌄ Queries
    ⌄ mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ⌄ Answers
    › mit.edu: type NS, class IN, ns ns1-37.akam.net
    › mit.edu: type NS, class IN, ns asia2.akam.net
    › mit.edu: type NS, class IN, ns ns1-173.akam.net
    › mit.edu: type NS, class IN, ns use5.akam.net
    › mit.edu: type NS, class IN, ns usw2.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 use2.akam.net
  ⌄ 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
    › use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    › 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
    › ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
    › ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    › ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    [Request In: 3]
    [Time: 0.016391000 seconds]
```

```
0000  f8 e4 e3 d8 24 30 40 b9  3c 45 60 de 08 00 45 00   ····$0@· <E`···E·
0010  01 b0 25 d8 00 00 37 11  9c 42 80 c1 0f 0d 0a f8   ··%···7· ·B······
0020  25 5d 00 35 cc de 01 9c  d9 00 00 02 81 80 00 01   %]·5···· ········
0030  00 08 00 00 00 0b 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01 c0 0c 00 02 00  01 00 00 07 08 00 11 06   ········ ········
0050  6e 73 31 2d 33 37 04 61  6b 61 6d 03 6e 65 74 00   ns1-37·a kam·net·
0060  c0 0c 00 02 00 01 00 00  07 08 00 08 05 61 73 69   ········ ·····asi
0070  61 32 c0 2c c0 0c 00 02  00 01 00 00 07 08 00 0a   a2·,···· ········
0080  07 6e 73 31 2d 31 37 33  c0 2c c0 0c 00 02 00 01   ·ns1-173 ·,······
0090  00 00 07 08 00 07 04 75  73 65 35 c0 2c c0 0c 00   ·······u se5·,···
00a0  02 00 01 00 00 07 08 00  07 04 75 73 77 32 c0 2c   ········ ··usw2·,
00b0  c0 0c 00 02 00 01 00 00  07 08 00 07 04 65 75 72   ········ ·····eur
00c0  35 c0 2c c0 0c 00 02 00  01 00 00 07 08 00 08 05   5·,····· ········
00d0  61 73 69 61 31 c0 2c c0  0c 00 02 00 01 00 00 07   asia1·,· ········
00e0  08 00 07 04 75 73 65 32  c0 2c c0 92 00 01 00 01   ····use2 ·,······
00f0  00 00 8c ab 00 04 17 4a  19 40 c0 b9 00 01 00 01   ·······J ·@······
0100  00 00 90 5a 00 04 60 07  31 40 c0 6c 00 01 00 01   ···Z··`· 1@·l····
0110  00 00 cd d6 00 04 02 10  28 40 c0 6c 00 1c 00 01   ········ (@·l····
0120  00 00 cd d6 00 10 26 00  14 03 00 0a 00 00 00 00   ······&· ········
0130  00 00 00 00 00 40 c0 7f  00 01 00 01 00 00 c3 d5   ·····@·· ········
0140  00 04 b8 1a a1 40 c0 a5  00 01 00 01 00 00 8b 7e   ·····@·· ·······~
0150  00 04 5f 64 af 40 c0 42  00 01 00 01 00 00 8d 4c   ··_d·@·B ·······L
0160  00 04 5f 65 24 40 c0 25  00 01 00 01 00 01 26 aa   ··_e$@·% ······&·
0170  00 04 c1 6c 5b 25 c0 25  00 1c 00 01 00 01 26 aa   ···l[%·% ······&·
0180  00 10 26 00 14 01 00 02  00 00 00 00 00 00 00 00   ··&····· ········
0190  00 25 c0 56 00 01 00 01  00 00 e0 97 00 04 c1 6c   ·%·V···· ·······l
01a0  5b ad c0 56 00 1c 00 01  00 00 e0 97 00 10 26 00   [··V···· ······&·
01b0  14 01 00 02 00 00 00 00  00 00 00 00 00 ad         ········ ······
```

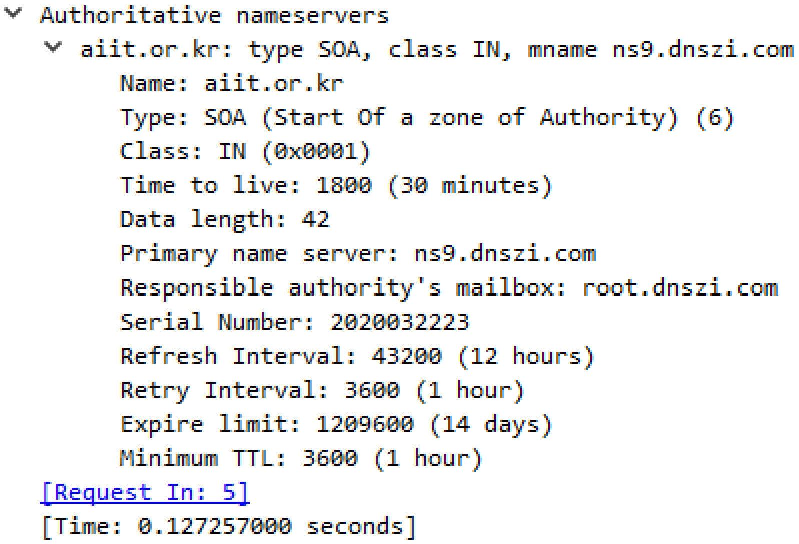
Text item (text), 28 bytes
Packets: 9 · Displayed: 9 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Figure 4 [S4]



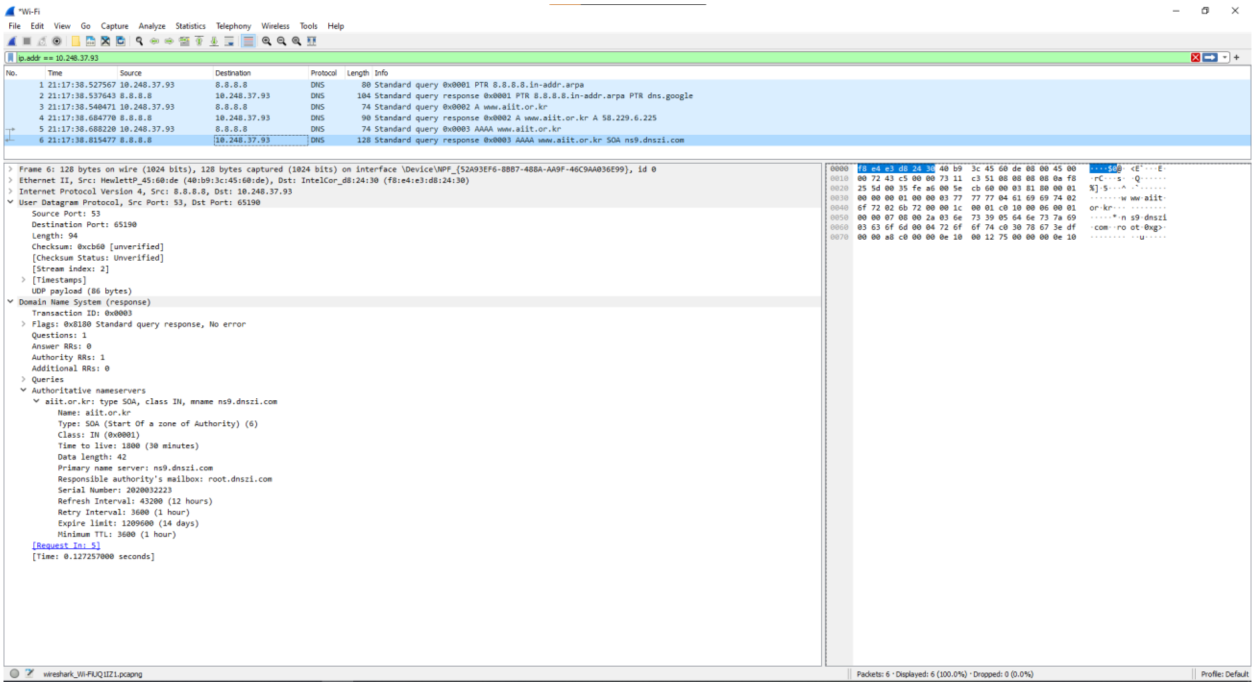
```
Queries
Answers
  8.8.8.8.in-addr.arpa: type PTR, class IN, dns.google
    Name: 8.8.8.8.in-addr.arpa
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
    Time to live: 16905 (4 hours, 41 minutes, 45 seconds)
    Data length: 12
    Domain Name: dns.google
[Request In: 1]
[Time: 0.010076000 seconds]
```

Figure 5 [S5]



```
Authoritative nameservers
  aiit.or.kr: type SOA, class IN, mname ns9.dnszi.com
    Name: aiit.or.kr
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 42
    Primary name server: ns9.dnszi.com
    Responsible authority's mailbox: root.dnszi.com
    Serial Number: 2020032223
    Refresh Interval: 43200 (12 hours)
    Retry Interval: 3600 (1 hour)
    Expire limit: 1209600 (14 days)
    Minimum TTL: 3600 (1 hour)
[Request In: 5]
[Time: 0.127257000 seconds]
```

Figure 6 [S6]


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.248.37.93
```

```
No.     Time            Source         Destination    Protocol Length Info
      1 21:17:38.527567 10.248.37.93   8.8.8.8        DNS         80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
      2 21:17:38.537643 8.8.8.8        10.248.37.93   DNS        104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
      3 21:17:38.540471 10.248.37.93   8.8.8.8        DNS         74 Standard query 0x0002 A www.aiit.or.kr
      4 21:17:38.684770 8.8.8.8        10.248.37.93   DNS         90 Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
      5 21:17:38.688220 10.248.37.93   8.8.8.8        DNS         74 Standard query 0x0003 AAAA www.aiit.or.kr
      6 21:17:38.815477 8.8.8.8        10.248.37.93   DNS        128 Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com
```

```
> Frame 6: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \Device\NPF_{52A93EF6-8BB7-488A-AA9F-46C9AA036E99}, id 0
> Ethernet II, Src: HewlettP_45:60:de (40:b9:3c:45:60:de), Dst: IntelCor_d8:24:30 (f8:e4:e3:d8:24:30)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.248.37.93
v User Datagram Protocol, Src Port: 53, Dst Port: 65190
    Source Port: 53
    Destination Port: 65190
    Length: 94
    Checksum: 0xcb60 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (86 bytes)
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  > Queries
  v Authoritative nameservers
    v aiit.or.kr: type SOA, class IN, mname ns9.dnszi.com
          Name: aiit.or.kr
          Type: SOA (Start Of a zone of Authority) (6)
          Class: IN (0x0001)
          Time to live: 1800 (30 minutes)
          Data length: 42
          Primary name server: ns9.dnszi.com
          Responsible authority's mailbox: root.dnszi.com
          Serial Number: 2020032223
          Refresh Interval: 43200 (12 hours)
          Retry Interval: 3600 (1 hour)
          Expire limit: 1209600 (14 days)
          Minimum TTL: 3600 (1 hour)
    [Request In: 5]
    [Time: 0.127257000 seconds]
```

```
0000  f8 e4 e3 d8 24 30 40 b9  3c 45 60 de 08 00 45 00   ····$0@· <E`···E·
0010  00 72 43 c5 00 00 73 11  c3 51 08 08 08 08 0a f8   ·rC···s· ·Q······
0020  25 5d 00 35 fe a6 00 5e  cb 60 00 03 81 80 00 01   %]·5···^ ·`······
0030  00 00 00 01 00 00 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
0040  6f 72 02 6b 72 00 00 1c  00 01 c0 10 00 06 00 01   or·kr··· ········
0050  00 00 07 08 00 2a 03 6e  73 39 05 64 6e 73 7a 69   ·····*·n s9·dnszi
0060  03 63 6f 6d 00 04 72 6f  6f 74 c0 30 78 67 3e df   ·com··ro ot·0xg>·
0070  00 00 a8 c0 00 00 0e 10  00 12 75 00 00 00 0e 10   ········ ··u·····
```

```
wireshark_Wi-FiUQ1IZ1.pcapng
Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
```

Figure 7 [S7]