

Astrid Delestine

1/26/2023

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 labels 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]

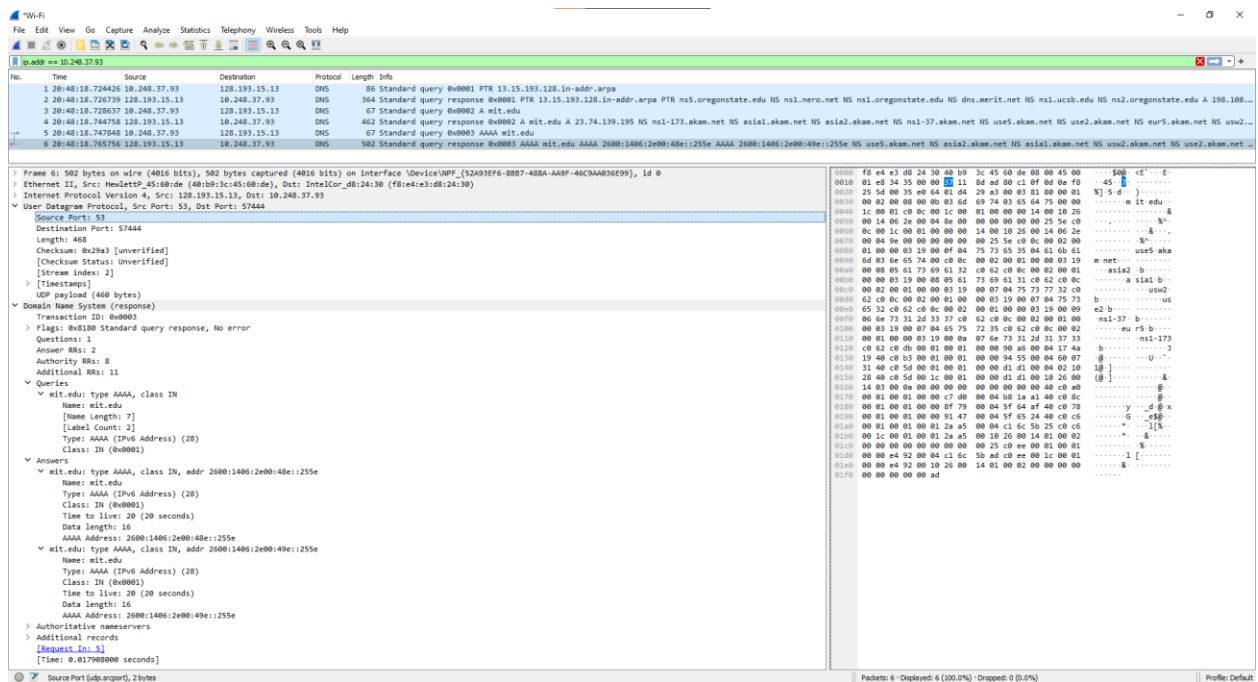


Figure 1 [S1]

▼ 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]

The image shows a Wireshark packet capture of a DNS response. The packet is a Standard query response (0x0002) from 10.240.37.93. The response contains 11 answers and 11 additional records. The answers are NS records for mit.edu pointing to various akam.net servers. The additional records include A and AAAA records for eur5.akam.net, use2.akam.net, use5.akam.net, usw2.akam.net, asia1.akam.net, asia2.akam.net, ns1-37.akam.net, ns1-173.akam.net, and use2.akam.net.

Packet 9: Displayed: 9 (100.0%) - Dropped: 0 (0.0%)

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
  ▼ aait.or.kr: type SOA, class IN, mname ns9.dnszi.com
    Name: aait.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]

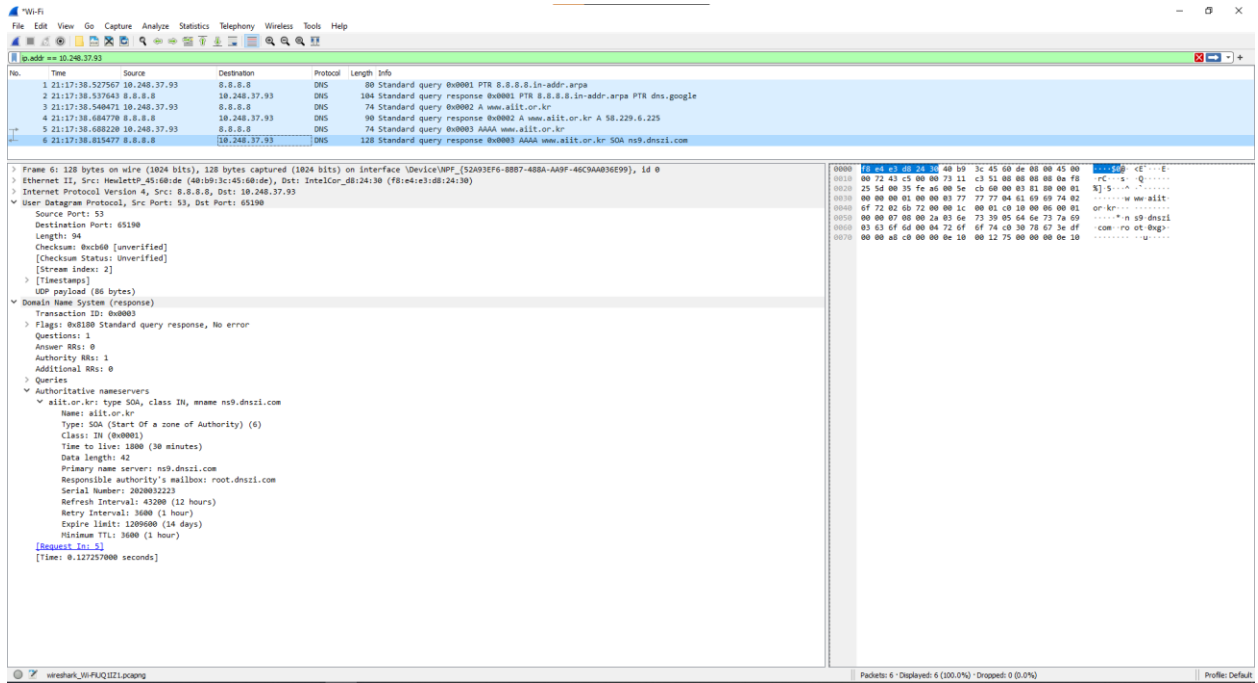


Figure 7 [S7]