

WIRESHARK LAB 2

mohammad Abaeiani

810198432

1.

```
C:\Windows\System32>nslookup www.google.com
Server: XiaoQiang
Address: 192.168.31.1

Non-authoritative answer:
Name:    www.google.com
Addresses: 2a00:1450:400f:804::2004
          142.250.74.132
```

Figure 1- nslookup response

When this command is run with a domain name as an argument it returns the ip address associated with the domain name. (it also returns the IPV6)

2.

```
C:\Windows\System32>nslookup -type=NS www.google.com
Server: XiaoQiang
Address: 192.168.31.1

DNS request timed out.
    timeout was 2 seconds.
google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 539600856
    refresh = 900 (15 mins)
    retry = 900 (15 mins)
    expire = 1800 (30 mins)
    default TTL = 60 (1 min)
```

Figure 2- NS response

nslookup -type=NS is a command used to specifically query the DNS namespace for Name Server records. This means that the command returns information about the nameservers that serve the domain you provided in the command.

3.

1134	6.624733	192.168.31.145	192.168.31.1	DNS	85 Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
1135	6.626467	192.168.31.1	192.168.31.145	DNS	108 Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa PTR XiaoQiang
1136	6.627343	192.168.31.145	192.168.31.1	DNS	74 Standard query 0x0002 A www.google.com
1139	6.629587	192.168.31.1	192.168.31.145	DNS	90 Standard query response 0x0002 A www.google.com A 142.250.74.132
1140	6.631851	192.168.31.145	192.168.31.1	DNS	74 Standard query 0x0003 AAAA www.google.com
1142	6.634011	192.168.31.1	192.168.31.145	DNS	102 Standard query response 0x0003 AAAA www.google.com AAAA 2a00:1450:400f:804::2004
2745	16.579992	192.168.31.145	192.168.31.1	DNS	85 Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
2747	16.582919	192.168.31.1	192.168.31.145	DNS	108 Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa PTR XiaoQiang
2748	16.583918	192.168.31.145	192.168.31.1	DNS	74 Standard query 0x0002 NS www.google.com
3022	18.598613	192.168.31.145	192.168.31.1	DNS	74 Standard query 0x0003 NS www.google.com
3050	18.771563	192.168.31.1	192.168.31.145	DNS	124 Standard query response 0x0003 NS www.google.com SOA ns1.google.com

Figure 3-DN queries

In the query sequence the first query is a request and if it times out this will be sent again and after that the server will send on or more packets containing the requested information.

4.

```

v Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    > www.google.com: type AAAA, class IN
  v Answers
    > www.google.com: type AAAA, class IN, addr 2a00:1450:400f:804::2004
    [Request In: 1140]
    [Time: 0.002160000 seconds]

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
  v Queries
    > www.google.com: type NS, class IN
  v Authoritative nameservers
    > google.com: type SOA, class IN, mname ns1.google.com
    [Request In: 3022]
    [Time: 0.172950000 seconds]

```

DNS query packets contain information about the domain name being queried and the type of query being made. The query packet is sent to the DNS server and contains a query ID, flags, the domain name being queried, the type of query (e.g. A, AAAA, MX, etc.), and other optional fields like the source port and additional record types. The DNS server responds to the query with one or more packet(s) containing the requested information.

5.

```

v Flags: 0x8180 Standard query response, No error
  1... .. = Response: Message is a response
  .000 0... .. = Opcode: Standard query (0)
  .... .0.. .. = Authoritative: Server is not an authority for domain
  .... .0. .... = Truncated: Message is not truncated
  .... ..1 .... = Recursion desired: Do query recursively
  .... ..1... .. = Recursion available: Server can do recursive queries
  .... ..0... .. = Z: reserved (0)
  .... ....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
  .... ....0 .... = Non-authenticated data: Unacceptable
  .... .... 0000 = Reply code: No error (0)

```

Figure 4- FLAGS

The flags contain some information about the state of the DNS response like: Type of the message, opcode, if the server is authoritative, if the message has errors and ...

```

  ▾ Answers
    ▾ www.google.com: type AAAA, class IN, addr 2a00:1450:400f:804::2004
      Name: www.google.com
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 78 (1 minute, 18 seconds)
      Data length: 16
      AAAA Address: 2a00:1450:400f:804::2004

```

Figure 5- Answers

The answers(which are contained in A and AAAA responses) contain different fields like Type, Class, TTL, length and address which give some information to the receiver.

6.

```

  ▾ google.com: type SOA, class IN, mname ns1.google.com
    Name: google.com
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 38
    Primary name server: ns1.google.com

```

Figure 6 - TTL

TTL is 60 seconds and it can be found in response packet(in this image it is response of the NS request)

HTTP:

1.

11789	4.955131	192.168.31.145	128.119.245.12	HTTP	432 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
12809	5.357472	128.119.245.12	192.168.31.145	HTTP	1355 HTTP/1.1 200 OK (text/html)
12860	5.388668	192.168.31.145	128.119.245.12	HTTP	389 GET /pearson.png HTTP/1.1
13457	5.585907	192.168.31.145	128.119.245.12	HTTP	389 GET /favicon.ico HTTP/1.1
13707	5.657354	192.168.31.145	178.79.137.164	HTTP	356 GET /8E_cover_small.jpg HTTP/1.1
13850	5.761046	128.119.245.12	192.168.31.145	HTTP	754 HTTP/1.1 200 OK (PNG)
14436	6.107040	178.79.137.164	192.168.31.145	HTTP	225 HTTP/1.1 301 Moved Permanently
14438	6.107040	128.119.245.12	192.168.31.145	HTTP	539 HTTP/1.1 404 Not Found (text/html)

There are 4 get requests

First one is for the html content:

11789	4.955131	192.168.31.145	128.119.245.12	HTTP	432 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
-------	----------	----------------	----------------	------	--

Next 3 are for the images and icons (2 images and one icon):

12860	5.388668	192.168.31.145	128.119.245.12	HTTP	389 GET /pearson.png HTTP/1.1
13457	5.585907	192.168.31.145	128.119.245.12	HTTP	389 GET /favicon.ico HTTP/1.1
13707	5.657354	192.168.31.145	178.79.137.164	HTTP	356 GET /8E_cover_small.jpg HTTP/1.1

2.

The response to the text request is like below(it is contained in line-based text):

```
Line-based text data: text/html (23 lines)
<html>\n
<head>\n
<title>Lab2-4 file: Embedded URLs</title>\n
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">\n
</head>\n
\n
<body bgcolor="#FFFFFF" text="#000000">\n
\n
<p>\n
 </p>\n
<p>This little HTML file is being served by gaia.cs.umass.edu. \n
It contains two embedded images. The image above, also served from the \n
gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. \n
The image of our 8th edition book cover below is stored at, and served from,\n
a WWW server kurose.cslash.net in France:</p>\n
<p align="left"></p>\n
And while we have your attention, you might want to take time to check out the\n
\t\t available open resources for this book at\n
\t\t <a href="http://gaia.cs.umass.edu/kurose_ross"> http://gaia.cs.umass.edu/kurose_ross</a>.\n
\n
</body>\n
</html>\n
```

The content of the png file is as below(Portable Network Graphics):

```
Portable Network Graphics
PNG Signature: 89504e470d0a1a0a
Image Header (IHDR)
  Len: 13
  Chunk: IHDR
  ..0. .... = Ancillary: This is a CRITICAL chunk
  .... ..0. .... = Private: This is a PUBLIC chunk
  .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy
  Width: 253
  Height: 199
  Bit Depth: 8
  Colour Type: Indexed-colour (3)
  Compression Method: Deflate (0)
  Filter Method: Adaptive (0)
  Interlace Method: No interlace (0)
  CRC: 0xe50aa505
> Palette (PLTE)
> Image data chunk (IDAT)
> Image Trailer (IEND)
```

The other Get requests got either moved permanently or not found:

```

  Line-based text data: text/html (7 lines)
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <html><head>\n
  <title>404 Not Found</title>\n
  </head><body>\n
  <h1>Not Found</h1>\n
  <p>The requested URL /favicon.ico was not found on this server.</p>\n
  </body></html>\n

  Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
  > Content-Length: 0\r\n
  Date: Tue, 13 Jun 2023 13:26:17 GMT\r\n
  Server: lighttpd/1.4.47\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.449686000 seconds]
  [Request in frame: 13707]
  [Request URI: http://kurose.cslash.net/8E_cover_small.jpg]
```