



# Wireshark Lab 2

By

Hamidreza Aliakbarykhoyi  
Computer Networks



## CONTENTS

introduction .....	2
question 1 .....	3
Q 1 part 1 .....	3
q2 part 2.....	5
Q1 part3 .....	6
q1 part4 .....	7
q1 part5 .....	8
q1 part6 .....	9
q1 part7 .....	10
Question 2 .....	11
q2 part1 .....	11
Q2 part2 .....	11
q2 part3 .....	12
status line .....	12
response header .....	12

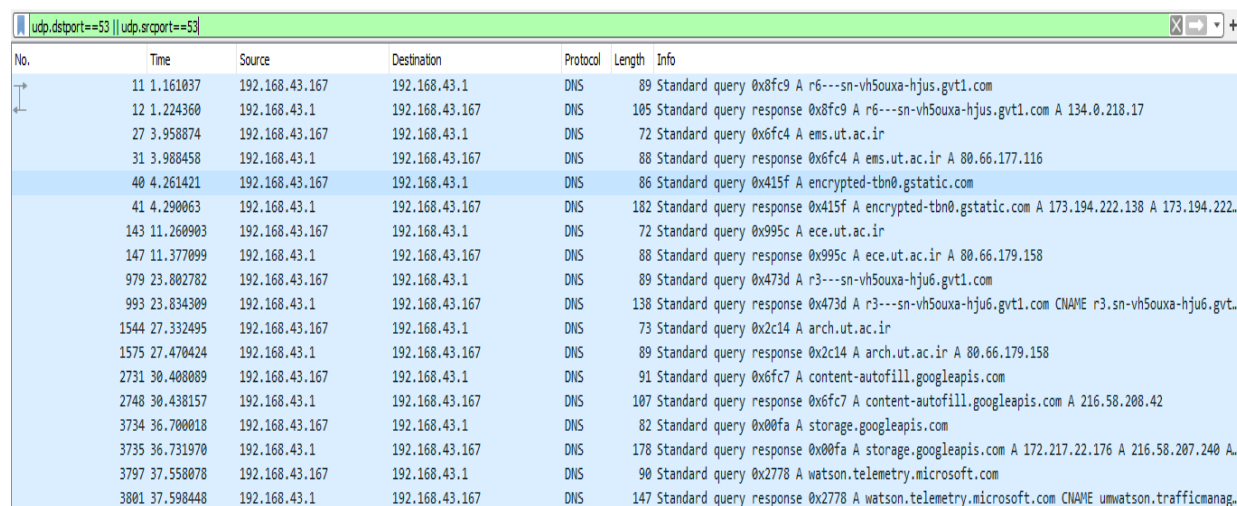
## INTRODUCTION

In this computer lab work we will learn more about two important application layer services that is DNS and HTTP services, as if we are going to talk about DNS in part one that we should run in to DNS queries and just explain what is the meaning of each type of query is. In the second part we will explain how GET messages work and what kind of functionality they bring to a way that it helps websites to load pages as we use our web-browsers.

## QUESTION 1

All we have to do is to talk about DNS:

### Q 1 PART 1



No.	Time	Source	Destination	Protocol	Length	Info
11	1.161837	192.168.43.167	192.168.43.1	DNS	89	Standard query 0x8fc9 A r6---sn-vh5ouxa-hjus.gvt1.com
12	1.224360	192.168.43.1	192.168.43.167	DNS	105	Standard query response 0x8fc9 A r6---sn-vh5ouxa-hjus.gvt1.com A 134.0.218.17
27	3.958874	192.168.43.167	192.168.43.1	DNS	72	Standard query 0x6fc4 A ems.ut.ac.ir
31	3.988458	192.168.43.1	192.168.43.167	DNS	88	Standard query response 0x6fc4 A ems.ut.ac.ir A 80.66.177.116
40	4.261421	192.168.43.167	192.168.43.1	DNS	86	Standard query 0x415f A encrypted-tbn0.gstatic.com
41	4.290063	192.168.43.1	192.168.43.167	DNS	182	Standard query response 0x415f A encrypted-tbn0.gstatic.com A 173.194.222.138 A 173.194.222...
143	11.268903	192.168.43.167	192.168.43.1	DNS	72	Standard query 0x995c A ece.ut.ac.ir
147	11.377099	192.168.43.1	192.168.43.167	DNS	88	Standard query response 0x995c A ece.ut.ac.ir A 80.66.179.158
979	23.802782	192.168.43.167	192.168.43.1	DNS	89	Standard query 0x473d A r3---sn-vh5ouxa-hju6.gvt1.com
993	23.834309	192.168.43.1	192.168.43.167	DNS	138	Standard query response 0x473d A r3---sn-vh5ouxa-hju6.gvt1.com CNAME r3.sn-vh5ouxa-hju6.gvt...
1544	27.332495	192.168.43.167	192.168.43.1	DNS	73	Standard query 0x2c14 A arch.ut.ac.ir
1575	27.470424	192.168.43.1	192.168.43.167	DNS	89	Standard query response 0x2c14 A arch.ut.ac.ir A 80.66.179.158
2731	30.408089	192.168.43.167	192.168.43.1	DNS	91	Standard query 0x6fc7 A content-autofill.googleapis.com
2748	30.438157	192.168.43.1	192.168.43.167	DNS	107	Standard query response 0x6fc7 A content-autofill.googleapis.com A 216.58.208.42
3734	36.700018	192.168.43.167	192.168.43.1	DNS	82	Standard query 0x00fa A storage.googleapis.com
3735	36.731970	192.168.43.1	192.168.43.167	DNS	178	Standard query response 0x00fa A storage.googleapis.com A 172.217.22.176 A 216.58.207.240 A...
3797	37.558078	192.168.43.167	192.168.43.1	DNS	90	Standard query 0x2778 A watson.telemetry.microsoft.com
3801	37.598448	192.168.43.1	192.168.43.167	DNS	147	Standard query response 0x2778 A watson.telemetry.microsoft.com CNAME umwatson.trafficmanag...

Figure 1

As we see in figure 1 we captured all DNS packets meanwhile we tried to load ece.ut.ac.ir as our destination website and in this part we are going to check it.

First DNS packet has sent from gvt1.com service redirector that

Redirector.**gvt1.com** technically is a redirection service employed by Google for informing users about upcoming updates and similar. ...

Redirector.**gvt1.com** virus is a term that might be used by users who have suffered from unpleasant activities that come from this website.

Second despite main ut.ac.ir domains we caught gstatic.com that

**Gstatic.com** is a reliable domain used by Google LLC to increase network speed for users.

**Gstatic.com** is a reliable domain used by Google LLC to increase network speed for users. **Gstatic** is not a virus, and a domain utilized by Google to host various static content, such as images, CSS, or JavaScript.

Third we captured googleapis.com that

**googleapis.com** is a legitimate service (API) provided by Google, however, many cyber criminals (scammers) use it to promote various 'tech' (technical) support scams. The purpose of these scams is to extort money from innocent people by tricking them into paying for certain services or products.

These services is sub-node of main-node servers that just boost the speed of accessibility to services and sites, locations are different whole over the world

The Transaction ID is a random number generated by the nameserver initiating the query. When the answering nameserver responds with an answer, it will set the same transaction ID.

## Q2 PART 2

```
> Frame 143: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{E6EFF515-5E15-4CEC-9E4E-2E6D4C459D81}, id 0
> Ethernet II, Src: IntelCor_5d:02:96 (60:36:dd:5d:02:96), Dst: XiaomiCo_06:35:d5 (a4:4b:d5:06:35:d5)
> Internet Protocol Version 4, Src: 192.168.43.167, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 56124, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x995c
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v ece.ut.ac.ir: type A, class IN
      Name: ece.ut.ac.ir
      [Name Length: 12]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 147]
```

```
0000 a4 4b d5 06 35 d5 60 36 dd 5d 02 96 08 00 45 00 ..K..5..6..]....E
0010 00 3a 53 b8 00 00 80 11 0f 02 c0 a8 2b a7 c0 a8 ..S.....+...
0020 2b 01 db 3c 00 35 06 26 fe c8 99 5c 01 00 00 01 +...<5&...\\....
0030 00 00 00 00 00 00 03 65 63 65 02 75 74 02 61 63 .....e ce-ut-ac
0040 02 69 72 00 00 01 00 01 .....ir.....
```

Figure 2

```
v 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
  v Queries
    v ece.ut.ac.ir: type A, class IN
      Name: ece.ut.ac.ir
      [Name Length: 12]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 147]
```

Figure 3

As we see in queries part we got type A that means it's a version 4 internet protocol and class IN refers to internet-network

```

  ▾ 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)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▾ Queries
    ▾ ece.ut.ac.ir: type A, class IN
      Name: ece.ut.ac.ir
      [Name Length: 12]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
    > Answers
      [Request In: 143]
      [Time: 0.116196000 seconds]

```

Figure 4

Figure 4 shows response message to ece.ut.ac.ir that request has shown in figure 3 .

### Q1 PART3

As we should talk about flags that are in response packet:

- First bit indicates that whether it is a response or a request.
  - Second opcode, shows the type of request that we have a query type here.
  - Because service is not an authoritative one of DNS that could be but it's not in this part. The DNS server is an Authoritative DNS for the domain and involves a copy of its domain information. This information can be passed to the DNS server by an administrator or the upper DNS server.
  - About being truncated we can say that because truncations happens when the message is longer than the standard limit issued for the Transport Layer protocol. TCP messages are length-unlimited but UDP messages have a maximum size of 512 bytes and messages longer than this size should be truncated.
- So this is not truncated.

-As for recursive method in flags we can say to the local DNS server holding destinations IP address, and moving backwards to deliver the IP to the clients local DNS). The Client request a Recursion Method using the Recursion Desired bits and the Server replies whether it supports the method by the Recursion Available bits or not.

-zbit is reserved for future updates and reuses.

- authority bit show that server has accepted the authorication or not

-reply code shows the reply of server that more common code of these kind are:

- NOERROR
- NXDOMAIN
- SERVFAIL
- REFUSED

These code are used to troubleshooting the server.

#### Q1 PART4

TTL stands for "Time to Live" . Its a metric for the time a DNS cache holds a record before discarding it in order to prevent slow cache access and high load. After the expiration of a records TTL, it should be discarded or refreshed .

TTL can be found in the Answers part of a Response message as shown below:



```

> Frame 147: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{E6EFF515-5E15-4CEC-9E4E-2E6D4C459D81}, id 0
> Ethernet II, Src: XiaomiCo_06:35:d5 (a4:4b:d5:06:35:d5), Dst: IntelCor_5d:02:96 (60:36:dd:5d:02:96)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.167
> User Datagram Protocol, Src Port: 53, Dst Port: 56124
▼ Domain Name System (response)
  Transaction ID: 0x995c
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ▼ Answers
    ▼ ece.ut.ac.ir: type A, class IN, addr 80.66.179.158
      Name: ece.ut.ac.ir
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20012 (5 hours, 33 minutes, 32 seconds)
      Data length: 4
      Address: 80.66.179.158
      [Request In: 143]
      [Time: 0.116196000 seconds]

```

*Figure 5*

As described and been proved in figure5.

## Q1 PART5

In this Lab we just talk about recursive type of queries that are for that:

In these types they are used in dns servers that in each request server searches for desired ip addresses that if it found though this will pass to source of request and ecen if it couldn't find any ipaddresses it will start a recursive query procedure to other local dns servers , contacting the local DNS, TLD's & Root DNS and vice versa in the destination side until it finds the Authoritative Name Server holding the corresponding IP address for the destination and returns it to the client. The procedure ends up by storing the recent accessed pair in the clients local DNS cache.

Questions: 1  
Answer RRs: 6  
Authority RRs: 0  
Additional RRs: 0

*Figure 6*

A resource record, commonly referred to as an RR, is the unit of information entered in DNS zone files; Resource records come in a fairly wide variety of types in order to provide extended name-resolution services.

Different types of RRs have different formats, as they contain different data. Many RRs share a common format. Each DNS Server contains RRs for the portion of the name space for which it is authoritative .

p.s:

as ece.ut.ac.ir didn't have RR's so I used googleaps.com RR .

## Q1 PART7

```
C:\Users\DELL>nslookup -type=NS ece.ut.ac.ir
Server: UnKnown
Address: 192.168.43.1

ut.ac.ir
      primary name server = utsrvns1.ut.ac.ir
      responsible mail addr = root.ut.ac.ir
      serial      = 2014020101
      refresh    = 3600 (1 hour)
      retry      = 1800 (30 mins)
      expire     = 2400000 (27 days 18 hours 40 mins)
      default TTL = 7200 (2 hours)
```

*Figure 7*

Primary name server shows that how it should get ip address of ece.ut.ac.ir and so the root server is root.ut.ac.ir that ece is a subdomain of it.

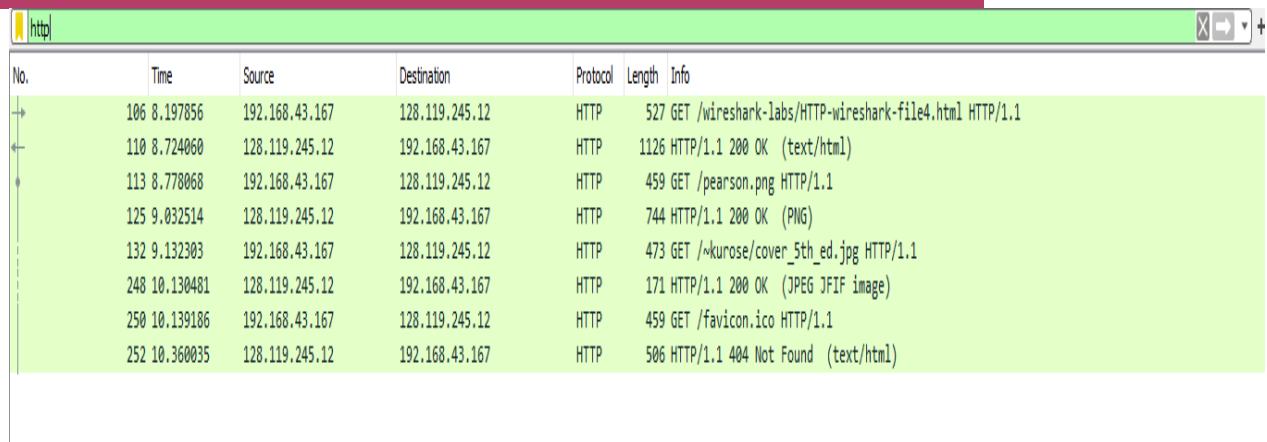
nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.

- The serial number is a specific property of a domain name, which the name server stores in the SOA (Start of Authority) record.

- which ip address is 192.168.43.1

- The domain or hosting expiry date can be fetched from the Client Login. Once logging into the Client login, Navigate through the menu Orders --> My Invoices. You will be able to find the list of invoices for your purchases. Do search for your domain name and find the expiry date.

## QUESTION 2



No.	Time	Source	Destination	Protocol	Length	Info
106	8.197856	192.168.43.167	128.119.245.12	HTTP	527	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
110	8.724060	128.119.245.12	192.168.43.167	HTTP	1126	HTTP/1.1 200 OK (text/html)
113	8.778068	192.168.43.167	128.119.245.12	HTTP	459	GET /pearson.png HTTP/1.1
125	9.032514	128.119.245.12	192.168.43.167	HTTP	744	HTTP/1.1 200 OK (PNG)
132	9.132303	192.168.43.167	128.119.245.12	HTTP	473	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
248	10.130481	128.119.245.12	192.168.43.167	HTTP	171	HTTP/1.1 200 OK (JPEG JFIF image)
250	10.139186	192.168.43.167	128.119.245.12	HTTP	459	GET /favicon.ico HTTP/1.1
252	10.360035	128.119.245.12	192.168.43.167	HTTP	506	HTTP/1.1 404 Not Found (text/html)

Figure 8

### Q2 PART1

As shown in figure 8 browser send 3 GET requests containing 1 text and 2 images. after that their all corresponding responses has been received from destination

### Q2 PART2

GET is a http request option that client can request for any part of webpages that are in http to server that server send corresponding data to it to user in this position we got 3 GET, 1 For test and 2 for images.

The server receives the request message, interprets and maps the *request-URI* to a document under its document directory. If the requested document is available, the server returns the document with a response status code "200 OK".

The response headers provide the necessary description of the document returned, such as the last-modified date. The response body contains the requested document.

```

v Hypertext Transfer Protocol
> GET /pearson.png HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36\r\n
Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,fa;q=0.8\r\n
\r\n

```

Figure 9

As shown in figure 9 in GET message for an image for corresponding webpage we used in http version 1.1 .

## Q2 PART3

The response message consist of two main parts as :

- Status line
- Response message

### STATUS LINE

It shows that with with versions we connected as in http:

- First is about HTTP version that here is 1.1 .
- Status code that has been generated by server to return of response that here is OK in 200.

### RESPONSE HEADER

It shows the resource data requested which in our case is the html text or the PNG, JPG files.

```

> Content-Length: 100968\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: image/jpeg\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.998178000 seconds]

```

Figure 10

Figure 10 shows an example of response header for an image.