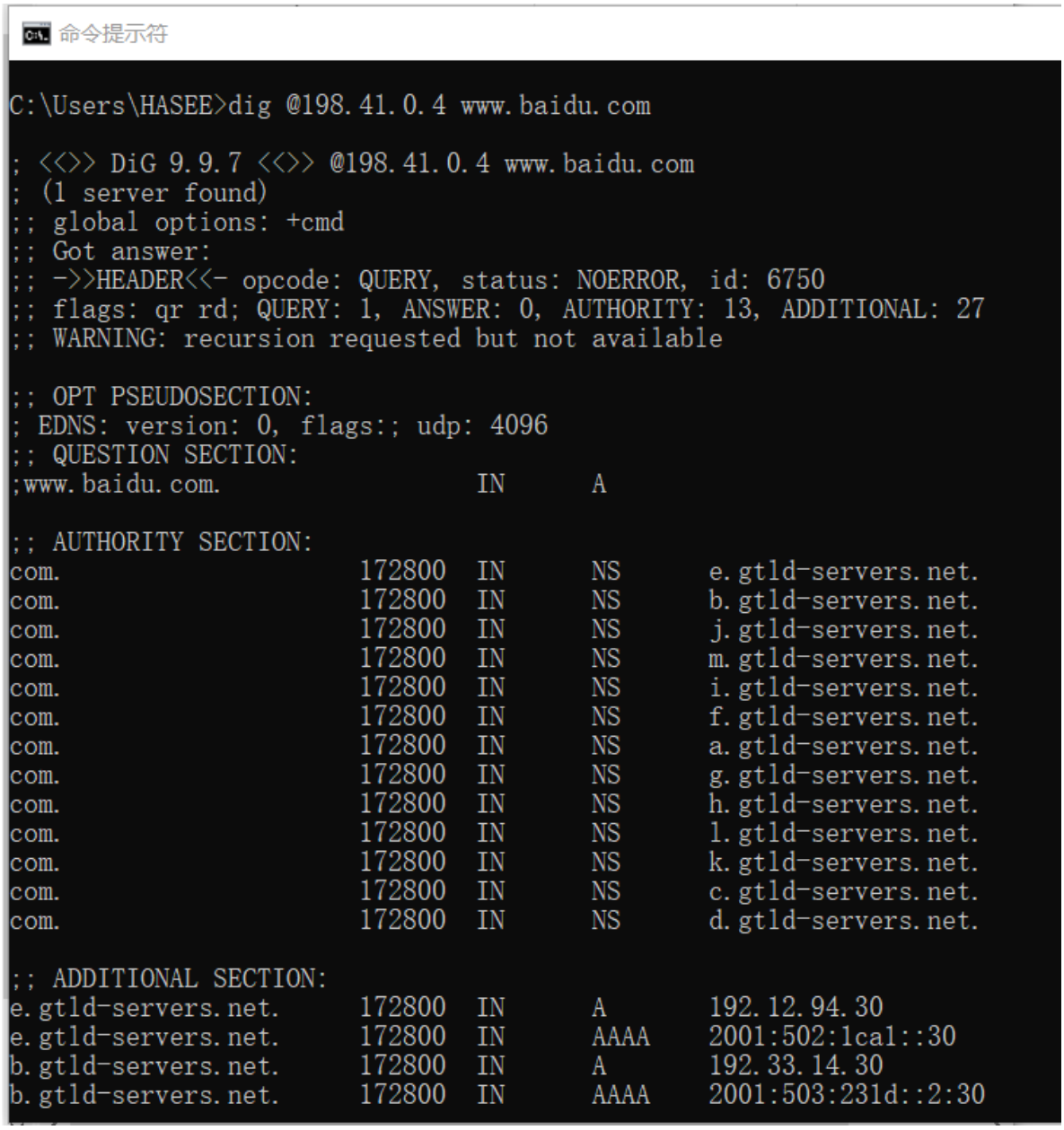
LAB-DNS 2020.5.4

Step 1: Manual Name Resolution

尝试手动解析www.baidu.com。

先找到它的一个ip:https://14.215.177.39。

先向指导中给出的一个“a"根域名服务器198.41.0.4 抛一个www.baidu.com的解析请求：



回复中没有给出www.baidu.com的完整ip，但是给出了可以解析"com"的一些域名服务器的ip:

比如第一个e.gtld-servers.net的ip是192.12.94.30。

尝试换用192.12.94.30继续解析www.baidu.com：

```
C:\Users\HASEE>dig @192.12.94.30 www.baidu.com

; <<>> DiG 9.9.7 <<>> @192.12.94.30 www.baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34032
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.baidu.com.                 IN      A

;; AUTHORITY SECTION:
baidu.com.              172800  IN      NS      ns2.baidu.com.
baidu.com.              172800  IN      NS      ns3.baidu.com.
baidu.com.              172800  IN      NS      ns4.baidu.com.
baidu.com.              172800  IN      NS      ns1.baidu.com.
baidu.com.              172800  IN      NS      ns7.baidu.com.

;; ADDITIONAL SECTION:
ns2.baidu.com.          172800  IN      A       220.181.33.31
ns3.baidu.com.          172800  IN      A       112.80.248.64
ns4.baidu.com.          172800  IN      A       14.215.178.80
ns1.baidu.com.          172800  IN      A       202.108.22.220
ns7.baidu.com.          172800  IN      A       180.76.76.92
```

这次也没有能直接得到www.baidu.com的域名，但是得到一些能解析"baidu.com"的域名服务器，选择用第一个220.181.33.31继续解析：

```
C:\Users\HASEE>dig @220.181.33.31 www.baidu.com

; <<>> DiG 9.9.7 <<>> @220.181.33.31 www.baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12119
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.baidu.com.                 IN      A

;; ANSWER SECTION:
www.baidu.com.          1200    IN      CNAME   www.a.shifen.com.

;; AUTHORITY SECTION:
a.shifen.com.           1200    IN      NS      ns3.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns2.a.shifen.com.
```

出了一个ANSWER SECTION：是www.a.shifen.com，查了一下这个网站：

http://shifen.com是百度当年为了竞价排名这个广告系统注册的，这个后台系统被命名为Shifen竞价排名，以前的销售系统现在还叫shifen销售系统。因为当年百度那个广告最低点击10分起价。为什么有这么一个奇怪的名字呢？在《相信中国》中，梁冬先生这样写道：“这个将来成就了百度80%收入的商业模式，最初的管理平台是由一个叫刘子正的实习生主持开发的。这也是唯一一个除http://baidu.com以外，外人所知的百度公司所拥有的国际域名。

貌似是百度弄得一个域名解析的保护壳，现在www.a.shifen.com已经无法访问了。估计国外的用户解析www.baidu.com的时候可能就会遇到这个问题。

那么继续换用www.a.shifen.com去解析一下：

```
C:\Users\HASEE>dig @192.5.6.30 www.a.shifen.com

; <<>> DiG 9.9.7 <<>> @192.5.6.30 www.a.shifen.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59115
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.a.shifen.com.              IN      A

;; AUTHORITY SECTION:
shifen.com.             172800  IN      NS      dns.baidu.com.
shifen.com.             172800  IN      NS      ns2.baidu.com.
shifen.com.             172800  IN      NS      ns3.baidu.com.
shifen.com.             172800  IN      NS      ns4.baidu.com.

;; ADDITIONAL SECTION:
dns.baidu.com.          172800  IN      A       202.108.22.220
```

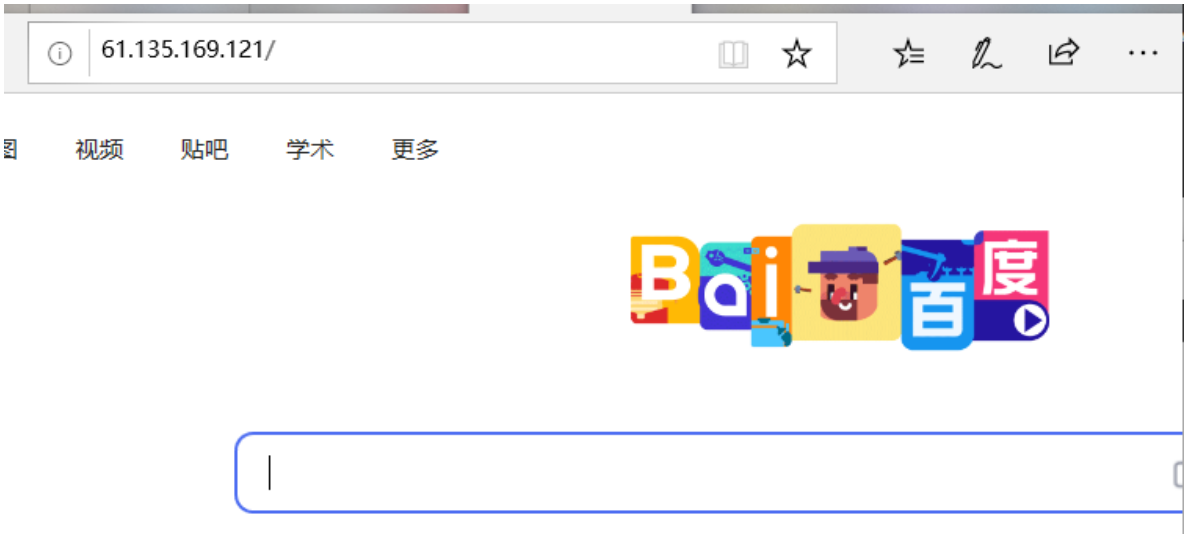
得到202.108.22.220，接下来只截取每次查询得到的ip了：

```
;; ADDITIONAL SECTION:
ns1.a.shifen.com.       1200    IN      A       61.135.165.224
```

得到域名解析ip61.135.165.224

```
;; ANSWER SECTION:
www.a.shifen.com.       300     IN      A       61.135.169.121
www.a.shifen.com.       300     IN      A       61.135.169.125
```

得到答案ip: 61.135.169.121,访问这个ip，得到的是百度的主页面：



所以这一次的解析能够成功得到百度的一个ip。

图就不画了，整理一下步骤吧：

1. 向198.41.0.4解析www.baidu.com，得到域名e.gtld-servers.net

   新域名能解析的域名后缀是com，新域名的ip是192.12.94.30

2. 向192.12.94.30解析www.baidu.com，得到域名ns2.baidu.com

   新域名能解析的域名后缀是baidu.com，新域名的ip是220.181.33.31

3. 向220.181.33.31解析www.baidu.com，得到答案域名www.a.shifen.com

   新域名能解析的域名后缀是www.baidu.com（？存疑，估计他的意思是说www.baidu.com就是指向www.a.shifen.com的意思），新域名没有给出ip，换用www.a.shifen.com去解析。

4. 向198.41.0.4（还是那个根域名服务器）解析www.a.shifen.com，得到域名a.gtld-servers.net

   新域名能解析的域名后缀是com，新域名的ip是192.5.6.30

5. 向192.5.6.30解析www.a.shifen.com，得到域名dns.baidu.com

   新域名能解析的域名后缀是shifen.com，新域名的ip是202.108.22.220

6. 向202.108.22.220解析www.a.shifen.com，得到域名ns3.a.shifen.com

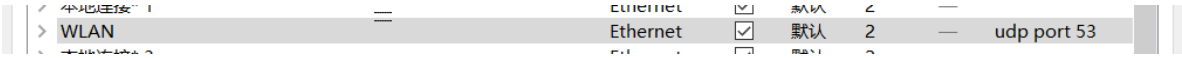
   新域名能解析的域名后缀是a.shifen.com，新域名的ip是61.135.165.224

7. 向61.135.165.224解析www.a.shifen.com，得到ip：61.135.169.121。

   访问61.135.169.121发现是百度的主页。

Step 2: Capture a Trace

设置filter



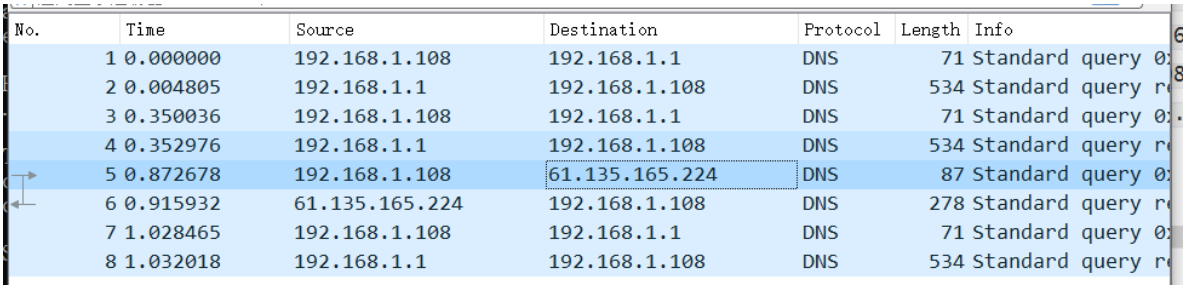
)

电脑用WLAN连接网络。

尝试解析命令并且捕获

运行`dig @61.135.165.224 www.a.shifen.com`

得到捕获结果：



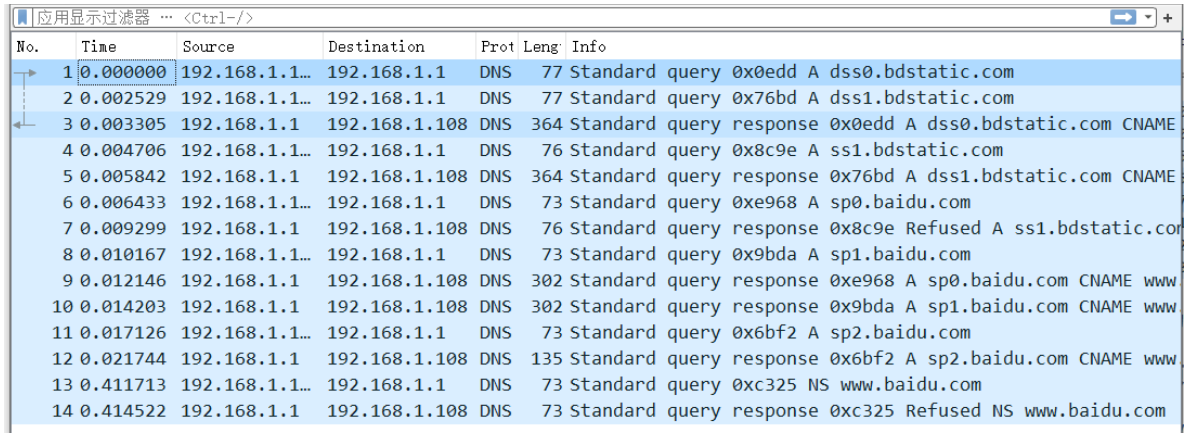
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.108	192.168.1.1	DNS	71	Standard query 0
2	0.004805	192.168.1.1	192.168.1.108	DNS	534	Standard query r
3	0.350036	192.168.1.108	192.168.1.1	DNS	71	Standard query 0
4	0.352976	192.168.1.1	192.168.1.108	DNS	534	Standard query r
5	0.872678	192.168.1.108	61.135.165.224	DNS	87	Standard query 0
6	0.915932	61.135.165.224	192.168.1.108	DNS	278	Standard query r
7	1.028465	192.168.1.108	192.168.1.1	DNS	71	Standard query 0
8	1.032018	192.168.1.1	192.168.1.108	DNS	534	Standard query r

应该是序号为5和6的是对应的解析请求，因为他俩含有61.135.165.224

尝试解析网页并且捕获

尝试访问www.baidu.com

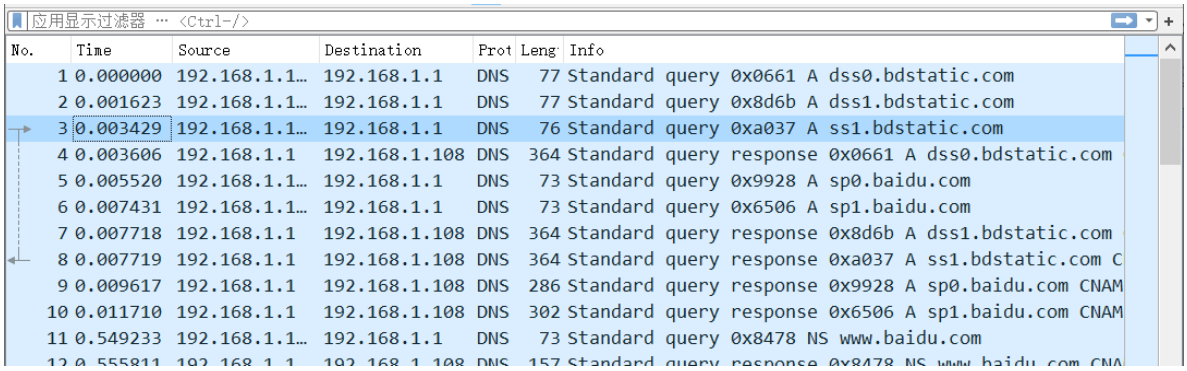
发现捕获了14条：



No.	Time	Source	Destination	Prot	Leng	Info
1	0.000000	192.168.1.1…	192.168.1.1	DNS	77	Standard query 0x0edd A dss0.bdstatic.com
2	0.002529	192.168.1.1…	192.168.1.1	DNS	77	Standard query 0x76bd A dss1.bdstatic.com
3	0.003305	192.168.1.1	192.168.1.108	DNS	364	Standard query response 0x0edd A dss0.bdstatic.com CNAME
4	0.004706	192.168.1.1…	192.168.1.1	DNS	76	Standard query 0x8c9e A ss1.bdstatic.com
5	0.005842	192.168.1.1	192.168.1.108	DNS	364	Standard query response 0x76bd A dss1.bdstatic.com CNAME
6	0.006433	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0xe968 A sp0.baidu.com
7	0.009299	192.168.1.1	192.168.1.108	DNS	76	Standard query response 0x8c9e Refused A ss1.bdstatic.com
8	0.010167	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0x9bda A sp1.baidu.com
9	0.012146	192.168.1.1	192.168.1.108	DNS	302	Standard query response 0xe968 A sp0.baidu.com CNAME www
10	0.014203	192.168.1.1	192.168.1.108	DNS	302	Standard query response 0x9bda A sp1.baidu.com CNAME www
11	0.017126	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0x6bf2 A sp2.baidu.com
12	0.021744	192.168.1.1	192.168.1.108	DNS	135	Standard query response 0x6bf2 A sp2.baidu.com CNAME www
13	0.411713	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0xc325 NS www.baidu.com
14	0.414522	192.168.1.1	192.168.1.108	DNS	73	Standard query response 0xc325 Refused NS www.baidu.com

尝试捕获大量的DNS流量

先打开baidu主页，再搜索test打开搜索页，再点击第一个百度翻译的页面后：



No.	Time	Source	Destination	Prot	Leng	Info
1	0.000000	192.168.1.1…	192.168.1.1	DNS	77	Standard query 0x0661 A dss0.bdstatic.com
2	0.001623	192.168.1.1…	192.168.1.1	DNS	77	Standard query 0x8d6b A dss1.bdstatic.com
3	0.003429	192.168.1.1…	192.168.1.1	DNS	76	Standard query 0xa037 A ss1.bdstatic.com
4	0.003606	192.168.1.1	192.168.1.108	DNS	364	Standard query response 0x0661 A dss0.bdstatic.com
5	0.005520	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0x9928 A sp0.baidu.com
6	0.007431	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0x6506 A sp1.baidu.com
7	0.007718	192.168.1.1	192.168.1.108	DNS	364	Standard query response 0x8d6b A dss1.bdstatic.com
8	0.007719	192.168.1.1	192.168.1.108	DNS	364	Standard query response 0xa037 A ss1.bdstatic.com C
9	0.009617	192.168.1.1	192.168.1.108	DNS	286	Standard query response 0x9928 A sp0.baidu.com CNAM
10	0.011710	192.168.1.1	192.168.1.108	DNS	302	Standard query response 0x6506 A sp1.baidu.com CNAM
11	0.549233	192.168.1.1…	192.168.1.1	DNS	73	Standard query 0x8478 NS www.baidu.com
12	0.555811	192.168.1.1	192.168.1.108	DNS	157	Standard query response 0x8478 NS www.baidu.com CNA

共捕获60条，保存在 中。

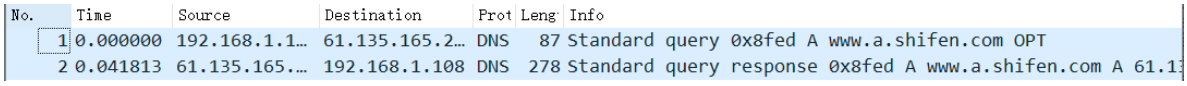
Step 3: Inspect the Trace

获取

还是看命令行的（因为比较少）

运行`dig @61.135.165.224 www.a.shifen.com`

得到：

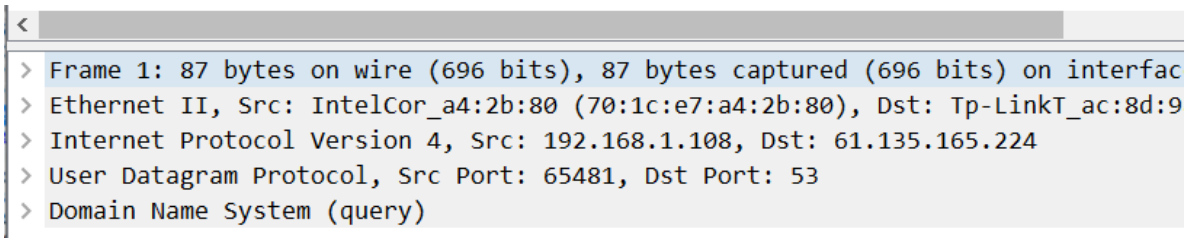


No.	Time	Source	Destination	Prot	Leng	Info
1	0.000000	192.168.1.1…	61.135.165.2…	DNS	87	Standard query 0x8fed A www.a.shifen.com OPT
2	0.041813	61.135.165.…	192.168.1.108	DNS	278	Standard query response 0x8fed A www.a.shifen.com A 61.1

观察DNS

查询DNS

协议



```
> Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interfac
> Ethernet II, Src: IntelCor_a4:2b:80 (70:1c:e7:a4:2b:80), Dst: Tp-LinkT_ac:8d:9
> Internet Protocol Version 4, Src: 192.168.1.108, Dst: 61.135.165.224
> User Datagram Protocol, Src Port: 65481, Dst Port: 53
> Domain Name System (query)
```

从上到下的协议分别是：Frame,Ethernet2,IPV4,UDP,DNS。

header

```
Info
Standard query 0x8fed A www.a.shifen.com OPT
Standard query response 0x8fed A www.a.shifen.com
```

发现发送和回复的header都是0x8fed

每一个所在的位置，高亮处：

```
Domain Name System (response)
    Transaction ID: 0x8fed
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 5
<
0000  70 1c e7 a4 2b 80 1c fa  68 ac 8d 98 08 00 45 00   p···+··· h·····E·
0010  01 08 2e dd 00 00 30 11  b5 8c 3d 87 a5 e0 c0 a8   ··.···0· ··=·····
0020  01 6c 00 35 ff c9 00 f4  98 91 8f ed 85 00 00 01   ·l·5···· ······
0030  00 02 00 05 00 05 03 77  77 77 01 61 06 73 68 69   ·······w ww·a·shi
0040  66 65 6e 03 63 6f 6d 00  00 01 00 01 c0 0c 00 01   fen·com· ·····
```

标志位

```
Domain Name System (query)
    Transaction ID: 0x8fed
  Flags: 0x0120 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)
      .... .... ..1. .... = AD bit: Set
<
0000  1c fa 68 ac 8d 98 70 1c  e7 a4 2b 80 08 00 45 00   ··h···p· ··+···E·
0010  00 49 74 10 00 00 80 11  21 18 c0 a8 01 6c 3d 87   ·It····· !····l=·
0020  a5 e0 ff c9 00 35 00 35  0f e3 8f ed 01 20 00 01   ·····5·5 ····· ··
```

Flags就是标志位，有很多位，不同的位表示不同的意思，比如第一位就是表示是不是query。高亮处就是储存的位置。

数量信息

```
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
> Queries
> Additional records
00  1c fa 68 ac 8d 98 70 1c  e7 a4 2b 80 08 00 45 00   ··h···p· ··+···E·
10  00 49 74 10 00 00 80 11  21 18 c0 a8 01 6c 3d 87   ·It····· !····l=·
20  a5 e0 ff c9 00 35 00 35  0f e3 8f ed 01 20 00 01   ·····5·5 ····· ··
30  00 00 00 00 00 01 03 77  77 77 01 61 06 73 68 69   ·······w ww·a·shi
```

查询的问题数1个。

查询信息

只有一个查询：

```
Queries
  www.a.shifen.com: type A, class IN
    Name: www.a.shifen.com
    [Name Length: 16]
    [Label Count: 4]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

其他信息

```
Additional records
  <Root>: type OPT
    Name: <Root>
    Type: OPT (41)
    UDP payload size: 4096
    Higher bits in extended RCODE: 0x00
    EDNS0 version: 0
  > Z: 0x0000
    Data length: 0
```

回复DNS，ip

上面查看的是查询的DNS包，下面换看回复的DNS包中的不同信息：

header

```
Flags: 0x8500 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .1.. .... .... = Authoritative: Server is an authority
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursive
    .... .... 0... .... = Recursion available: Server can't do r
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
```

这一次第一位是1，指Response类型。

数量信息

```
Questions: 1
Answer RRs: 2
Authority RRs: 5
Additional RRs: 5
> Queries
> Answers
```

有一个问题，两个回复。

回复信息（Answers)

```
Answers
  www.a.shifen.com: type A, class IN, addr 61.135.169.125
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 61.135.169.125
  www.a.shifen.com: type A, class IN, addr 61.135.169.121
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 61.135.169.121
```

回复了两个ip：61.135.169.125和61.135.169.121

回复DNS,下一个域名服务器

刚才的回复DNS是最后一次的查询（能马上得到ip)，现在看一下非最后一次的解析（得到的是下一次推荐的域名解析服务器）

捕获命令`dig @202.108.22.220 www.a.shifen.com`的DNS包。

回复信息

```
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 5
  Additional RRs: 6
  Queries
  Authoritative nameservers
    a.shifen.com: type NS, class IN, ns ns4.a.shifen.com
        Name: a.shifen.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1200 (20 minutes)
        Data length: 6
        Name Server: ns4.a.shifen.com
    a.shifen.com: type NS, class IN, ns ns3.a.shifen.com
```

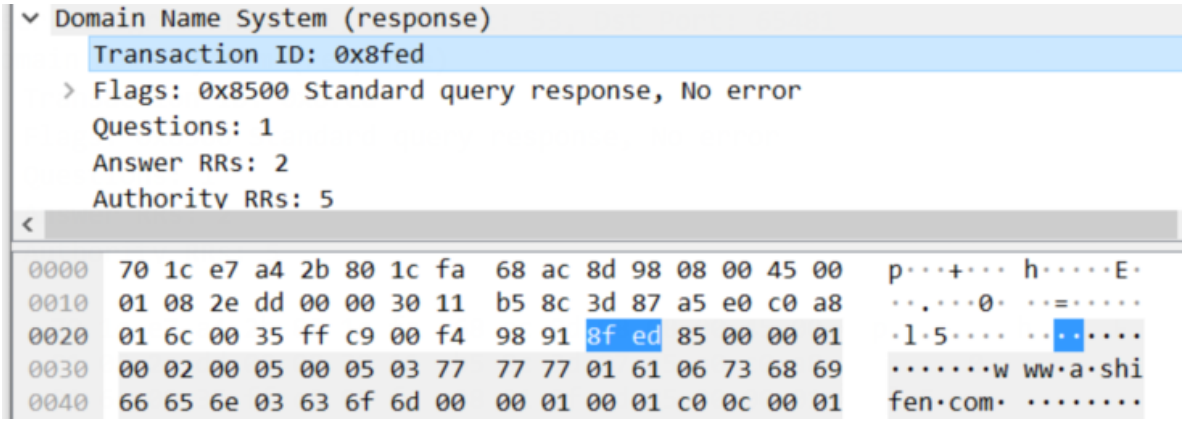
与前一个回复相比：

1. 没有Answer RRs.
2. 有Authority RRs: 共5个，提供了一些能解析a.shifen.com的域名及其ip。

Step 4: Details of DNS Messages

还是看命令`dig @61.135.165.224 www.a.shifen.com`的DNS的一个询问、一个回复包：

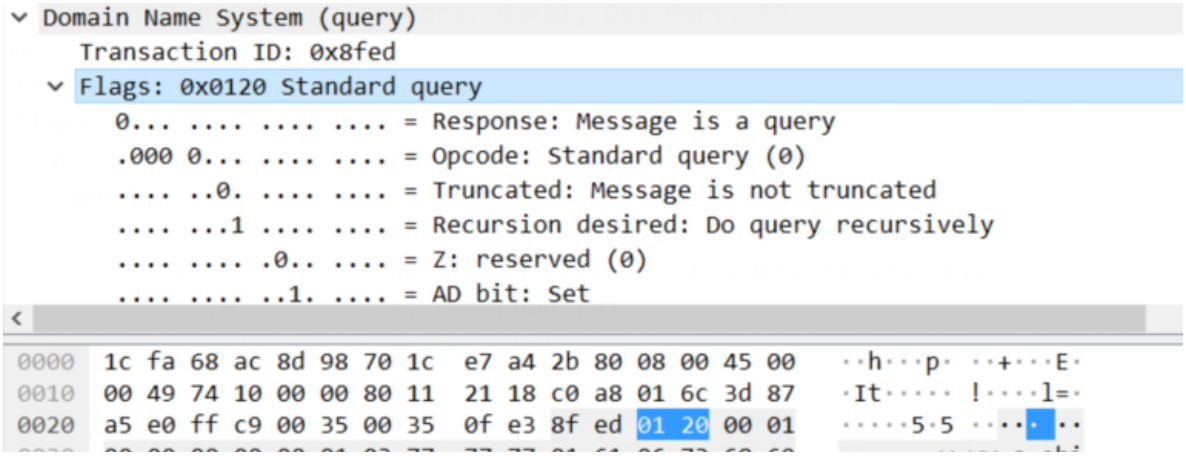
问题1



可以看到高亮部分就对应了Transaction ID，共占了32位。32位可以表达2^32=4e9种不同的ID，所以任意两次事务ID（随机选取）重复的可能性是1/4e9=2.5e-10。

此后也是依靠高亮的部分来数出对应部分所占的位数，就不一一截图了。

问题2



表示DNS类型的是Flags的第一位。0表示询问，1表示接受。

问题3

DNS的头包涵Transaction ID(2 bytes)、Flags(2 bytes)、四个数量(8 bytes)，所以总共是

12字节。

问题4

```
Authoritative nameservers
  a.shifen.com: type NS, class IN, ns ns3.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1200 (20 minutes)
      Data length: 6
      Name Server: ns3.a.shifen.com
  a.shifen.com: type NS, class IN, ns ns4.a.shifen.com
      Name: a.shifen.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 1200 (20 minutes)
```

域名服务器的域名储存在Name Server字段中，它管辖的域名后缀储存在Name中。这些储存在Authoritative nameservers中。

问题5

```
Additional records
  ns1.a.shifen.com: type A, class IN, addr 61.135.165.224
      Name: ns1.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 600 (10 minutes)
      Data length: 4
      Address: 61.135.165.224
  ns2.a.shifen.com: type A, class IN, addr 220.181.33.32
      Name: ns2.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

域名服务器的ip储存在Address字段中。它储存在Additional records中。

问题6

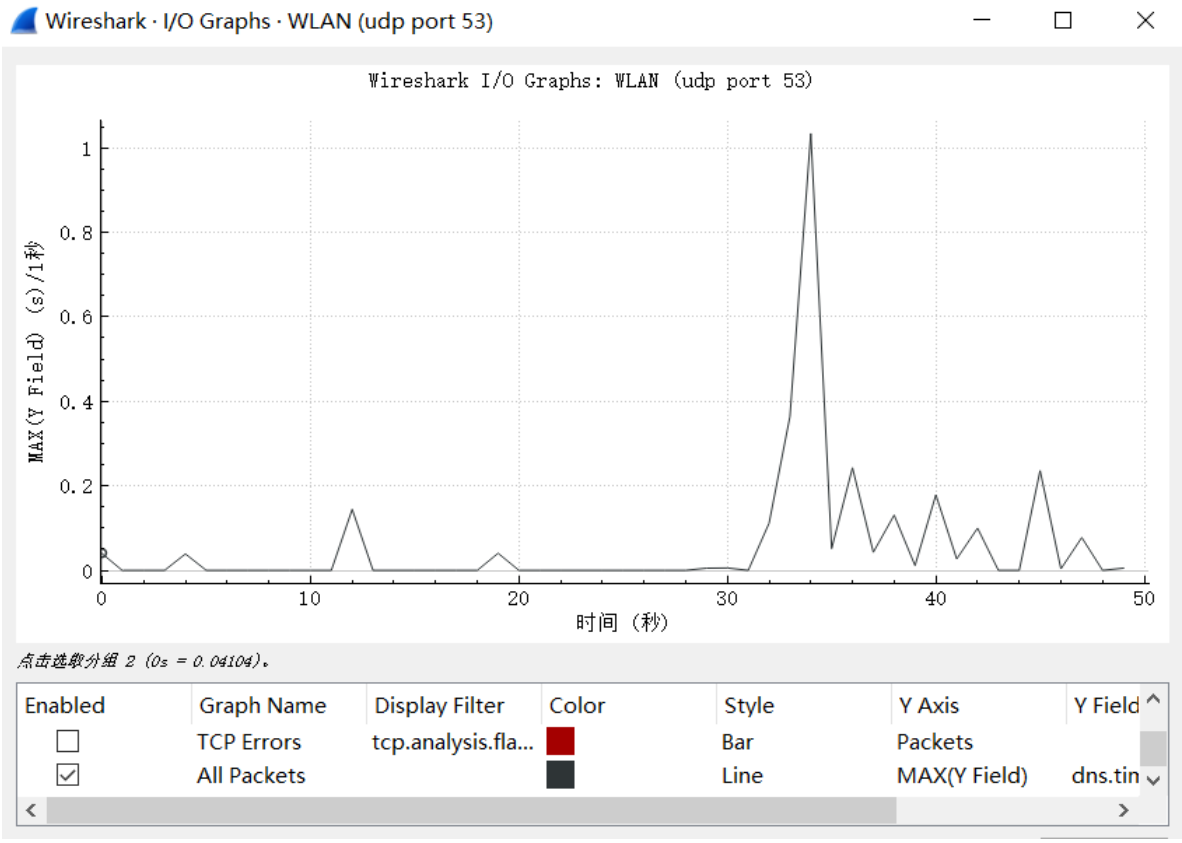
```
Answers
    www.a.shifen.com: type A, class IN, addr 61.135.169.125
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 61.135.169.125
    www.a.shifen.com: type A, class IN, addr 61.135.169.121
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 61.135.169.121
```

答案域名的ip储存在Address字段中。它储存在Answers中。

Step 5:DNS Response Time

先进行重新捕获数据（之前的都删掉了）：大概的做法是先用几次dig命令，然后等待10秒后，打开一些网页进行访问。

然后画图：



可以看到前几次（20秒之前的）就是dig命令的延迟时间。后几次（30秒之后）是访问网页的时间。

点击曲线，会在wire shark中选取到对应最近的包的信息行。