《计算机网络》实验报告（7）

Wireshark Lab: DNS

专　　业　软件工程

姓　　名　郭　政

学　　号　2023141461076

指导老师　程艳红

成绩分数

二零二五 年 五 月 二十七 日

Wireshark Lab: DNS

1. Run nslookup to obtain the IP address of a Web server in Asia. What is its IP address?
nslookup www.baidu.com
IP 地址是：110.242.69.21；110.242.70.57

```
C:\Users\13929>nslookup www.baidu.com
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
名称:    www.a.shifen.com
Addresses:  110.242.69.21
          110.242.70.57
Aliases:  www.baidu.com
```

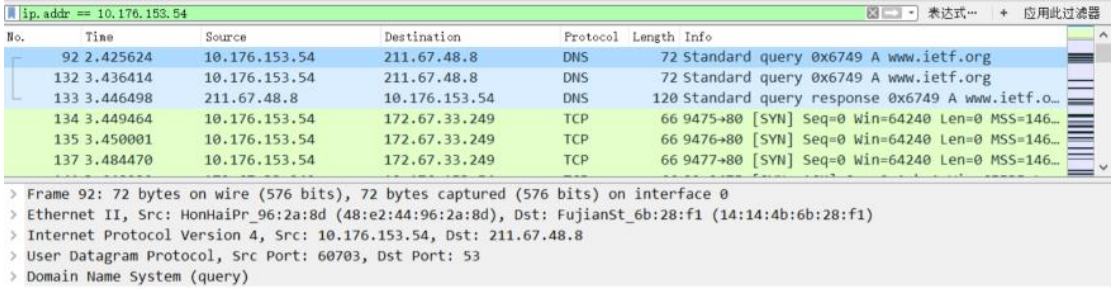
2. Run nslookup to determine the authoritative DNS servers for a university in Europe. What is its IP address.
nslookup -type=NS ox.ac.uk
IP 地址是：192.168.43.1

```
C:\Users\13929>nslookup -type=NS ox.ac.uk
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
ox.ac.uk        nameserver = dns2.ox.ac.uk
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk
ox.ac.uk        nameserver = dns0.ox.ac.uk
ox.ac.uk        nameserver = dns1.ox.ac.uk
```

3. 用 DNS 服务器查询 Yahoo! Mail 的邮件服务器

```
C:\Users\13929>nslookup -type=MX yahoo.com 8.8.8.8
服务器:  dns.google
Address:  8.8.8.8

非权威应答:
yahoo.com       MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com       MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
```

4. DNS 查询/响应是用 UDP 还是 TCP?
用的是 UDP 协议
5. DNS 查询消息的目的端口和响应消息的源端口？
DNS 查询消息的目的端口：53
DNS 响应消息的源端口：也是 53



```
C:\Users\13929>ipconfig -all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : LAPTOP-196TL048
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   物理地址. . . . . . . . . . . . . : BC-EC-A0-07-3F-21
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
```

```
C:\Users\13929>ipconfig /displaydns

Windows IP 配置

    osfsr.lenovomm.com
    ----------------------------------------
    记录名称. . . . . . . . : osfsr.lenovomm.com
    记录类型. . . . . . . . : 5
    生存时间. . . . . . . . : 7614
    数据长度. . . . . . . . : 8
    部分. . . . . . . . . . : 答案
    CNAME 记录  . . . . . . : fsrcn.lenovomm.com


    osfsr.lenovomm.com
    ----------------------------------------
    没有 AAAA 类型的记录


    记录名称. . . . . . . . : osfsr.lenovomm.com
    记录类型. . . . . . . . : 5
    生存时间. . . . . . . . : 8185
    数据长度. . . . . . . . : 8
    部分. . . . . . . . . . : 答案
    CNAME 记录  . . . . . . : fsrcn.lenovomm.com
```

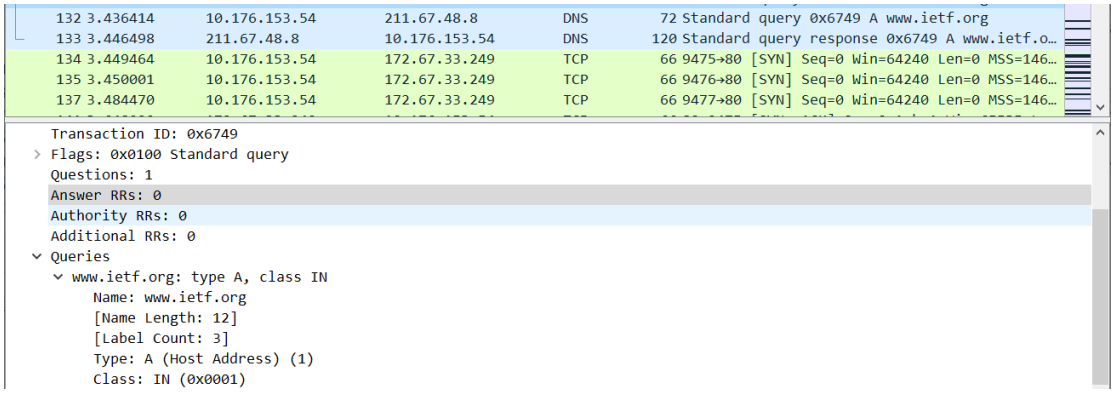
6. DNS 查询消息发往的 IP 是否与本地 DNS 相同？

   DNS 查询消息发送到的 IP 地址是 211.67.48.8。

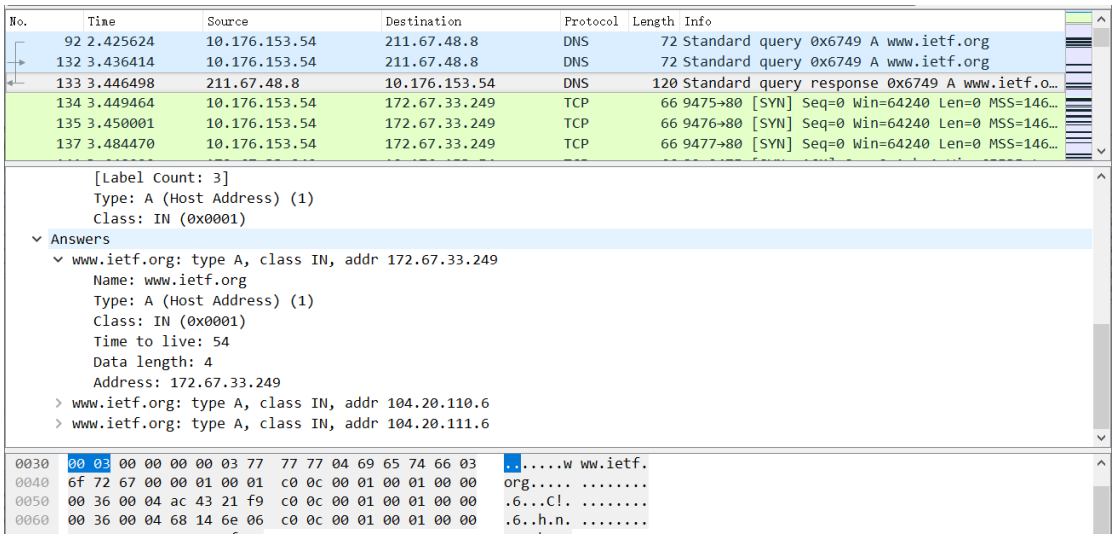
   使用 ipconfig 得到的本地 DNS 服务器地址也是 211.67.48.8，两者一致

7. 查询消息的类型是什么？是否包含 answers？

   消息类型为 A；没有包含任何 answer



8. 响应消息中有多少 answers？都包含了什么内容？



有 3 个答案包含以下信息：

主机名称、地址类型、类、TTL、数据长度和 IP 地址等信息

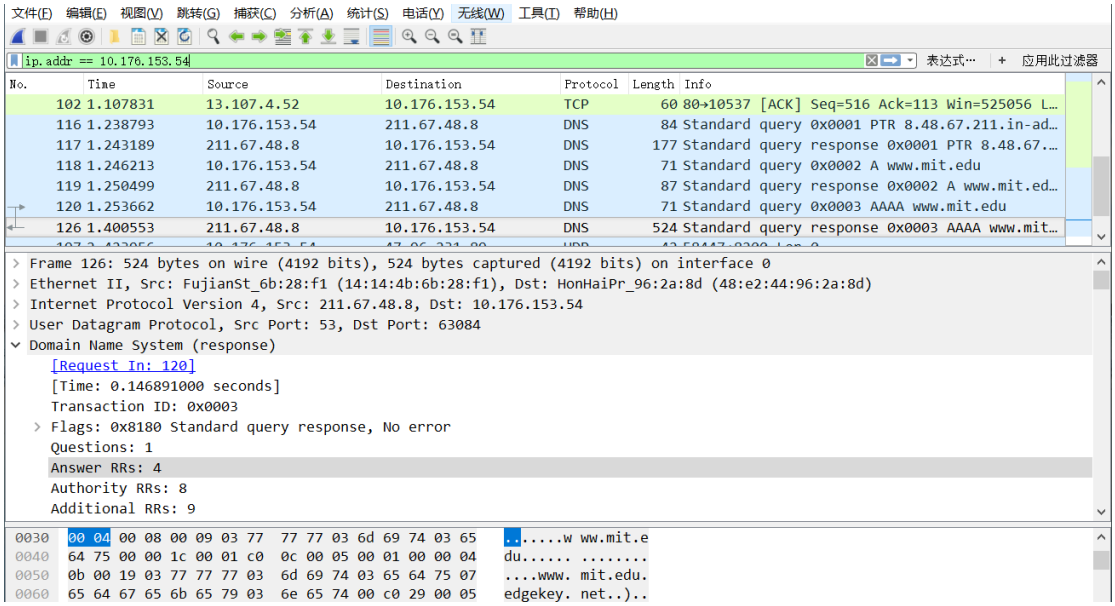
9. TCP SYN 包的目的 IP 是否在 DNS 响应中？

TCP SYN 包的目的 IP 不在 DNS 响应中

10. 网页中包含图片时，是否为每张图片重新发起 DNS 查询？

若图片域名已缓存，则不触发新的查询，若不在缓存中则发起查询

11. DNS 查询的目的端口和响应的源端口？



DNS 查询的目标端口是 53，DNS 响应的源端口也是 53

12. 查询发送到哪个 IP？是否是默认本地 DNS？

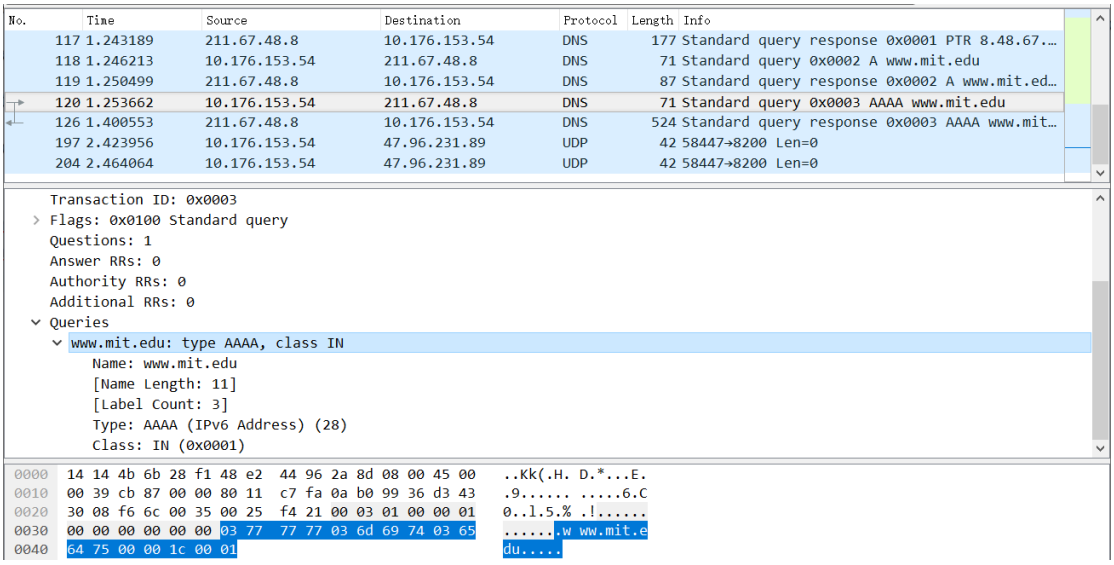
它被发送到 211.67.48.8，这是默认的本地 DNS 服务器

13. 查询类型？是否有 answers？

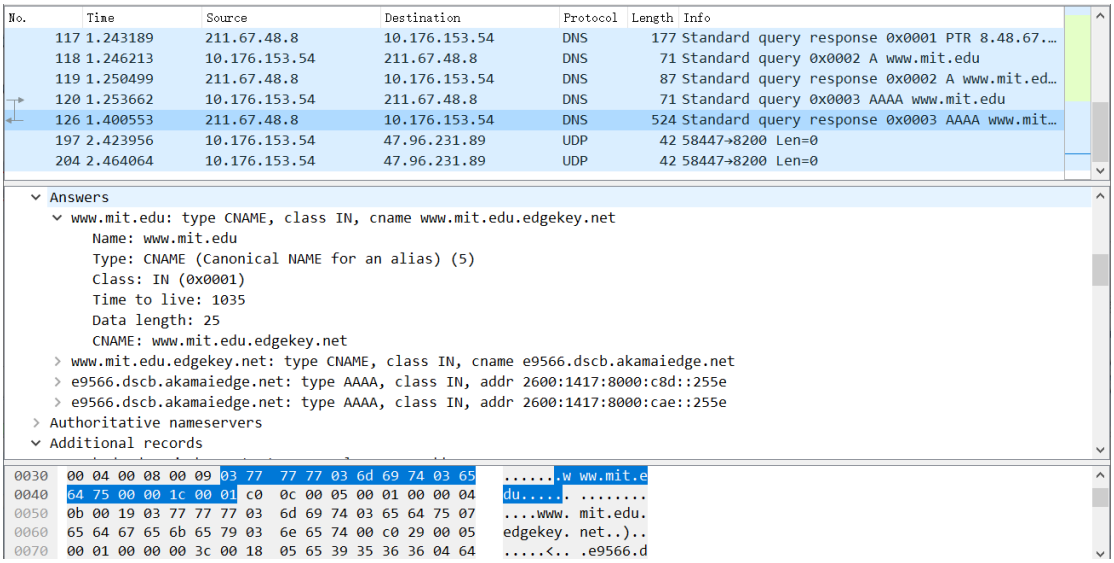
查询类型是 AAAA 类型，该查询消息不包含 answer

14. 响应中有多少 answers？都包含什么？

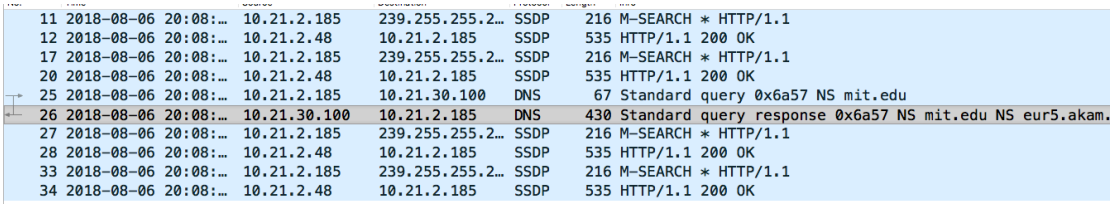
3 个 answer，该答案包括：主机名、地址类型、地址类别，以及 IP 地址



15. 提供截图



16. 查询消息发往哪个 IP？是默认 DNS 吗？
    是默认 DNS
17. 查询类型？是否有 answers?
    查询类型是 NS 类型，不包含任何 answer
18. 响应中提供了哪些 MIT 名称服务器？是否提供了其 IP?
    提供了大概 10 个，具体结果如下图
19. 提供截图



```
▸ Ethernet II, Src: HuaweiTe_b4:29:e1 (34:b3:54:b4:29:e1), Dst: Apple_ce:46:2d (ac:bc:32:ce:46:2d)
▸ Internet Protocol Version 4, Src: 10.21.30.100, Dst: 10.21.2.185
▸ User Datagram Protocol, Src Port: 53, Dst Port: 49594
▾ Domain Name System (response)
    Transaction ID: 0x6a57
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 10
  ▾ 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 eur5.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▸ mit.edu: type NS, class IN, ns asia2.akam.net
    ▸ mit.edu: type NS, class IN, ns usw2.akam.net
    ▸ mit.edu: type NS, class IN, ns asia1.akam.net
    ▸ mit.edu: type NS, class IN, ns use5.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-37.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
    ▸ 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
    ▸ usw2.akam.net: type A, class IN, addr 184.26.161.64
    ▸ asia1.akam.net: type A, class IN, addr 95.100.175.64
    ▸ use5.akam.net: type A, class IN, addr 2.16.40.64
    ▸ use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
```

20. 查询消息发往哪个 IP？是否是默认 DNS？若不是，对应什么？

No.	Time	Source	Destination	Protocol	Length	Info
48	1.424289	10.176.153.54	211.67.48.8	DNS	73	Standard query 0x83b0 A bitsy.mit.edu
53	1.453822	10.176.153.54	211.67.48.8	DNS	73	Standard query 0x83b0 A bitsy.mit.edu
54	1.459599	211.67.48.8	10.176.153.54	DNS	89	Standard query response 0x83b0 A bitsy.mit.…
55	1.462642	10.176.153.54	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr…
78	2.173767	10.176.153.54	47.96.231.89	UDP	42	58447→8200 Len=0
120	3.477643	10.176.153.54	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
139	4.039722	10.176.153.54	39.97.4.86	TLSv1.2	273	Application Data

DNS 第一次查询消息发送的 IP 地址是默认的本地域名服务器，查询到 bitsy.mit.edu 的 IP 地址：18.72.0.3，之后向这个 IP 地址发送查询消息，但失败了，因为 MIT 的这个 DNS 服务器已停用

21. 查询类型？是否有 answers?

查询类型是 A 类型，该查询消息不包含任何答案

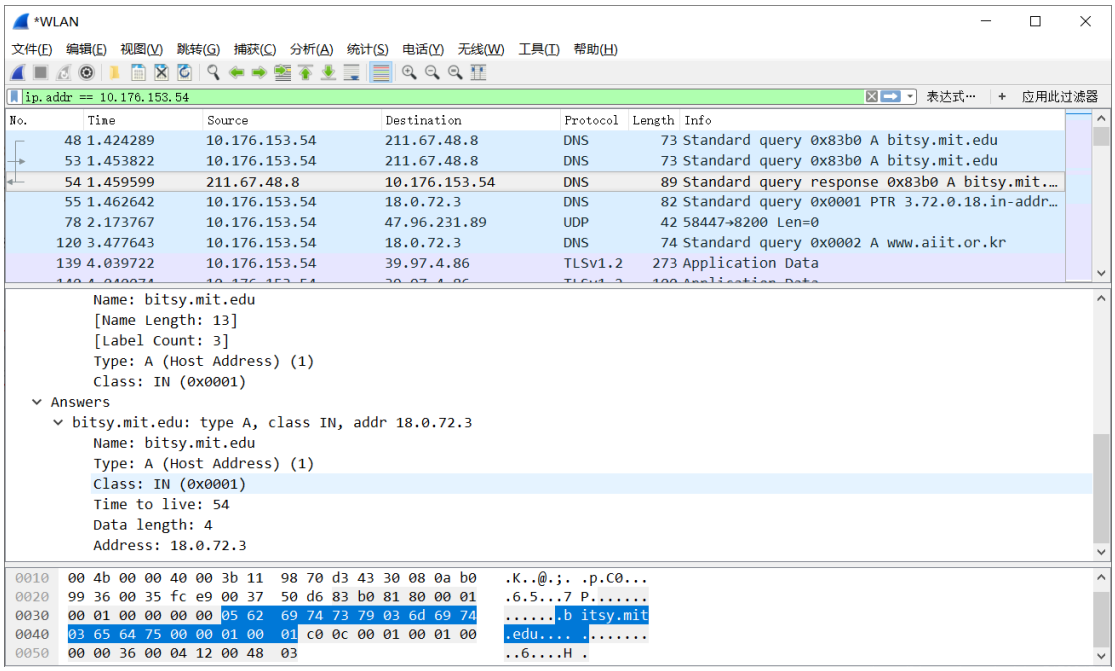
22. 响应中有多少 answers？都包含了什么？

没有 answer

No.	Time	Source	Destination	Protocol	Length	Info
19	2018-08-06 20:31:…	10.21.2.185	10.21.30.100	DNS	73	Standard query 0x7f9a A bitsy.mit.edu
20	2018-08-06 20:31:…	10.21.30.100	10.21.2.185	DNS	89	Standard query response 0x7f9a A bitsy.mit.edu
21	2018-08-06 20:31:…	10.21.2.185	18.72.0.3	DNS	74	Standard query 0x5fc5 A www.aiit.or.kr
46	2018-08-06 20:31:…	10.21.2.185	18.72.0.3	DNS	74	Standard query 0x5fc5 A www.aiit.or.kr
76	2018-08-06 20:31:…	10.21.2.185	18.72.0.3	DNS	74	Standard query 0x5fc5 A www.aiit.or.kr
10…	2018-08-06 20:34:…	10.21.2.185	10.21.30.100	DNS	98	Standard query 0x548f PTR lb._dns-sd._udp.0.2.
10…	2018-08-06 20:34:…	10.21.30.100	10.21.2.185	DNS	175	Standard query response 0x548f No such name PT

```
▸ Frame 76: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: Apple_ce:46:2d (ac:bc:32:ce:46:2d), Dst: HuaweiTe_b4:29:e1 (34:b3:54:b4:29:e1)
▸ Internet Protocol Version 4, Src: 10.21.2.185, Dst: 18.72.0.3
▸ User Datagram Protocol, Src Port: 64657, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x5fc5
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.aiit.or.kr: type A, class IN
        Name: www.aiit.or.kr
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

23. 提供截图


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
ip.addr == 10.176.153.54
表达式… + 应用此过滤器
No. Time Source Destination Protocol Length Info
48 1.424289 10.176.153.54 211.67.48.8 DNS 73 Standard query 0x83b0 A bitsy.mit.edu
53 1.453822 10.176.153.54 211.67.48.8 DNS 73 Standard query 0x83b0 A bitsy.mit.edu
54 1.459599 211.67.48.8 10.176.153.54 DNS 89 Standard query response 0x83b0 A bitsy.mit.…
55 1.462642 10.176.153.54 18.0.72.3 DNS 82 Standard query 0x0001 PTR 3.72.0.18.in-addr…
78 2.173767 10.176.153.54 47.96.231.89 UDP 42 58447→8200 Len=0
120 3.477643 10.176.153.54 18.0.72.3 DNS 74 Standard query 0x0002 A www.aiit.or.kr
139 4.039722 10.176.153.54 39.97.4.86 TLSv1.2 273 Application Data
Name: bitsy.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 54
Data length: 4
Address: 18.0.72.3
0010 00 4b 00 00 40 00 3b 11 98 70 d3 43 30 08 0a b0 .K..@.;. .p.C0...
0020 99 36 00 35 fc e9 00 37 50 d6 83 b0 81 80 00 01 .6.5...7 P.......
0030 00 01 00 00 00 00 05 62 69 74 73 79 03 6d 69 74 ....b itsy.mit
0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu.... ....
0050 00 00 36 00 04 12 00 48 03 ..6....H .