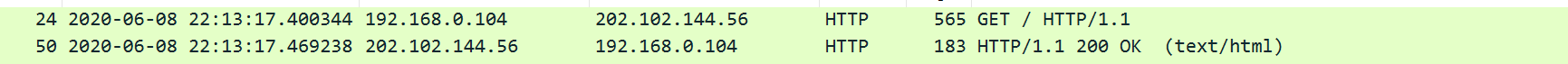
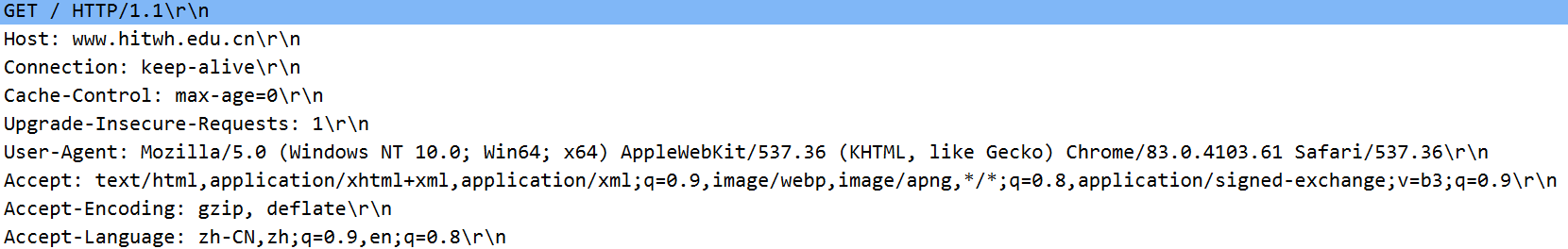
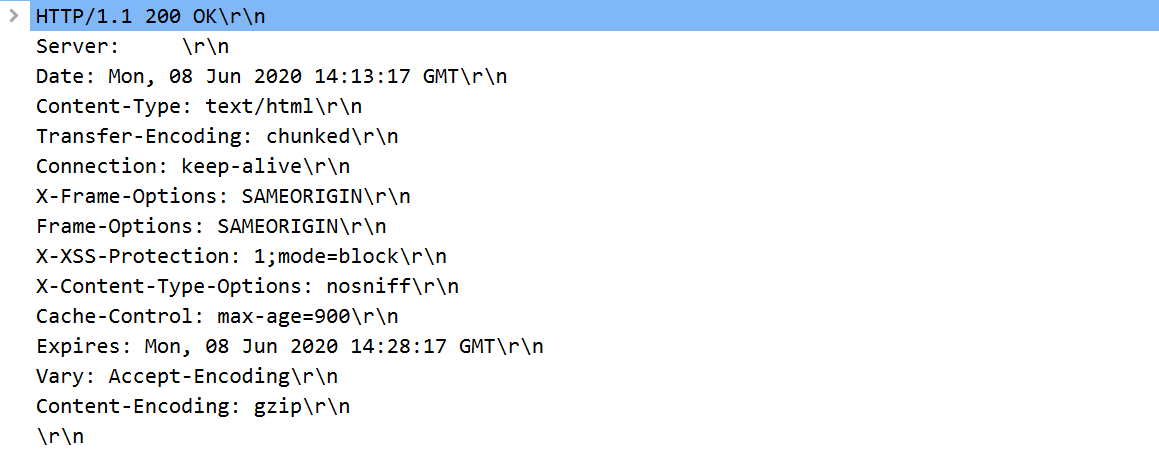
|  |  |
| --- | --- |
| **1** | 198.41.0.4 |
| **2** | 199.9.14.201 |
| **3** | 192.33.4.12 |
| **4** | 199.7.91.13 |
| **5** | 192.203.230.10 |
| **6** | 192.5.5.241 |
| **7** | 192.112.36.4 |
| **8** | 198.97.190.53 |
| **9** | 192.36.148.17 |
| **10** | 192.58.128.30 |
| **11** | 193.0.14.129 |
| **12** | 199.7.83.42 |
| **13** | 202.12.27.33 |

1. 列出在第7 步中分组列表子窗口所显示的所有协议类型。ARP HTTP UDP TCP DNS
2. 从发出HTTP GET 报文到接收到HTTP OK 响应报文共需要多长时间？（在默认的情况下，分组列表窗口中Time 列的值是从Wireshark 开始追踪到分组被俘获的总的时间数，以秒为单位。若要按time-of-day 格式显示Time 列的值，需选择View 下拉菜单，再选择Time Display Format，然后选择Time-of-day。）

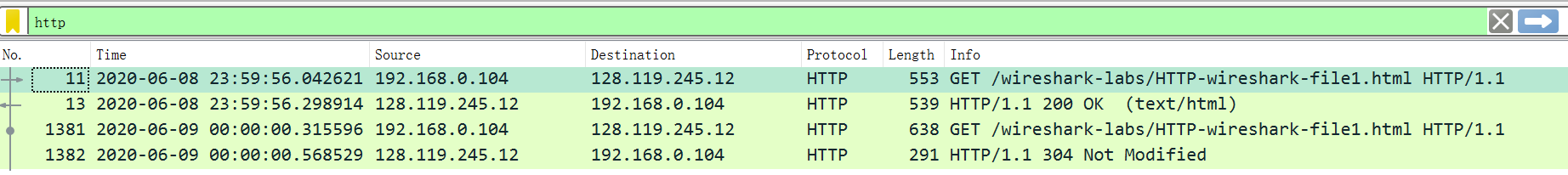


1. 你主机的IP 地址是什么？你所访问的主页所在服务器的IP 地址是什么？
2. 写出两个第9 步所显示的HTTP 报文头部行信息。





实验五



（1）你的浏览器运行的是HTTP1.0，还是HTTP1.1？你所访问的服务器所运行的HTTP 版本

号是多少？ HTTP1.1 HTTP 1.1

（2）你的浏览器向服务器指出它能接收何种语言版本的对象？

zh,en

（3）你的计算机的IP 地址是多少？服务器gaia.cs.umass.edu 的IP 地址是多少？

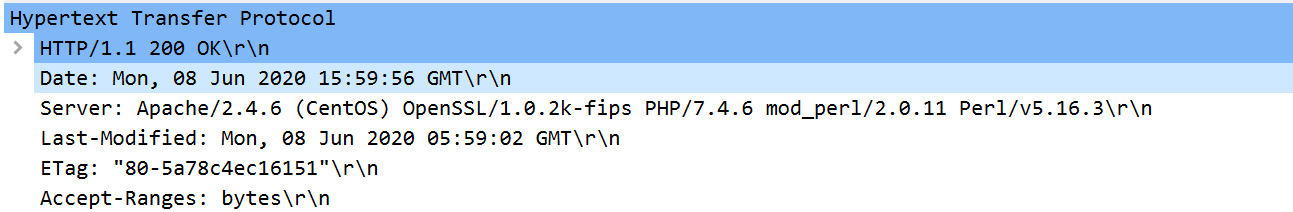
192.168.0.104; 128.119.245.12

（4）从服务器向你的浏览器返回的状态代码是多少？

200 OK

（5）你从服务器上所获取的HTML 文件的最后修改时间是多少？

Mon, 08 Jun 2020 05:59:02 GMT\r\n

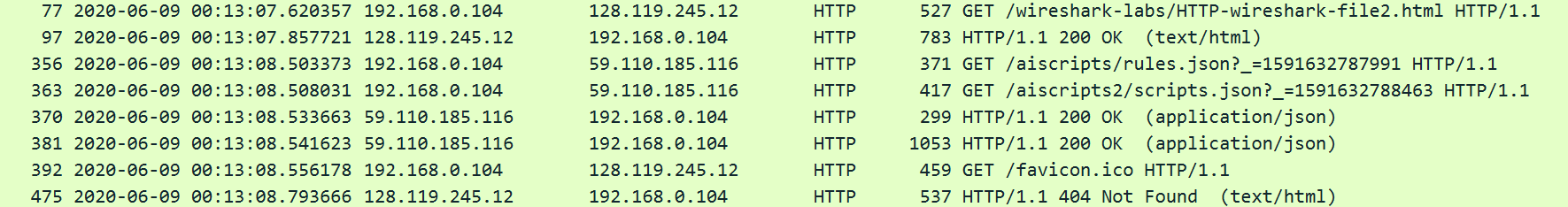


（6）返回到你的浏览器的内容一供多少字节？

128



------------------------------------------------------------------------



（7）分析你的浏览器向服务器发出的第一个HTTP GET 请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？

否

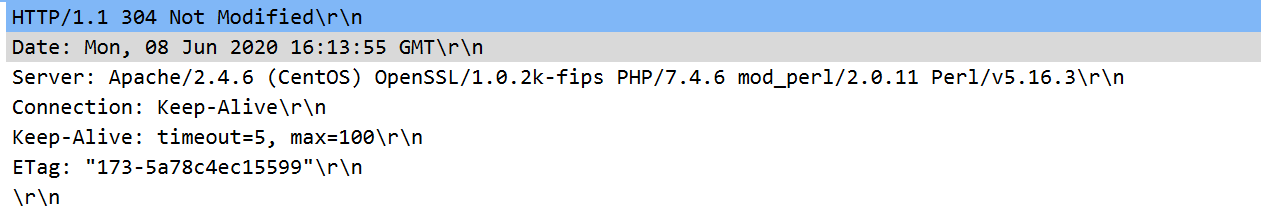
（8）分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？

有 HTTP/1.1 200 OK (text/html) 表明返回了文件的内容

（9）分析你的浏览器向服务器发出的第二个“HTTP GET”请求，在该请求报文中是否有一

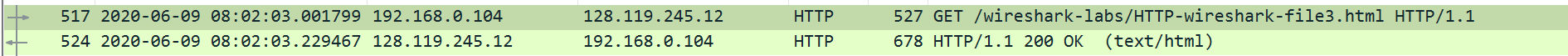
行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？

有 Date: Mon, 08 Jun 2020 16:13:55 GMT\r\n



（10）服务器对第二个HTTP GET 请求的响应中的HTTP 状态代码是多少？服务器是否明确返回了文件的内容？请解释。

没有。服务器返回了304表示之前发过的包没有修改不继续发了。



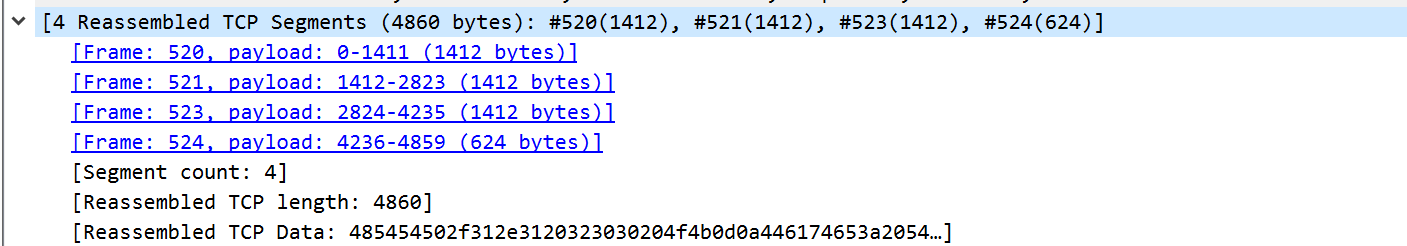
------------------------------------------------------------------------

（11）你的浏览器一共发出了多少个HTTP GET 请求？

1个

（12）承载这一个HTTP 响应报文一共需要多少个data-containing TCP 报文段？

4个



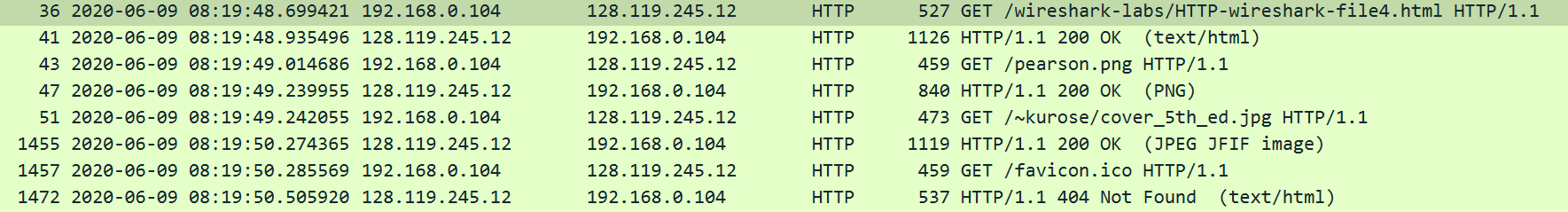
（13）与这个HTTP GET 请求相对应的响应报文的状态代码和状态短语是什么？



------------------------------------------------------------------------

（14）你的浏览器一共发出了多少个HTTP GET 请求？这些请求被发送到的目的地的IP 地址是多少？

4；目的ip：128.119.245.12



（15）浏览器在下载这两个图片时，是串行下载还是并行下载？请解释

串行下载。浏览器每次GET请求得到响应之后再发下一个GET请求

------------------------------------------------------------------------

（16）对于浏览器发出的最初的HTTP GET 请求，服务器的响应是什么(状态代码和状态短语)?

HTTP/1.1 401 Unauthorized\r\n



（17）当浏览器发出第二个HTTP GET 请求时，在HTTP GET 报文中包含了哪些新的字段？



----------------------------------------------------------------

（18）定位到DNS 查询报文和查询响应报文，这两种报文的发送是基于UDP 还是基于TCP

的？

UDP

（19）DNS 查询报文的目的端口号是多少？DNS 查询响应报文的源端口号是多少？

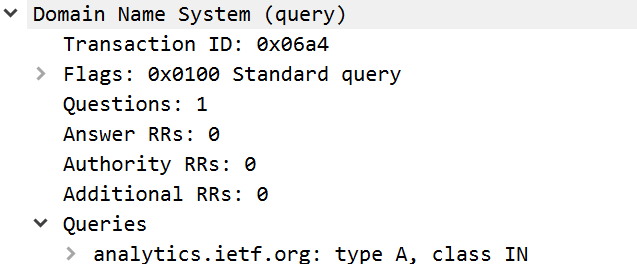
53；53

（20） DNS 查询报文发送的目的地的IP 地址是多少？利用ipconfig 命令（ipconfig/all）

决定你主机的本地DNS 服务器的IP 地址。这两个地指相同吗？

114.114.114.114; 一样

（21）检查DNS 查询报文，它是哪一类型的DNS 查询？该查询报文中包含“answers”吗？

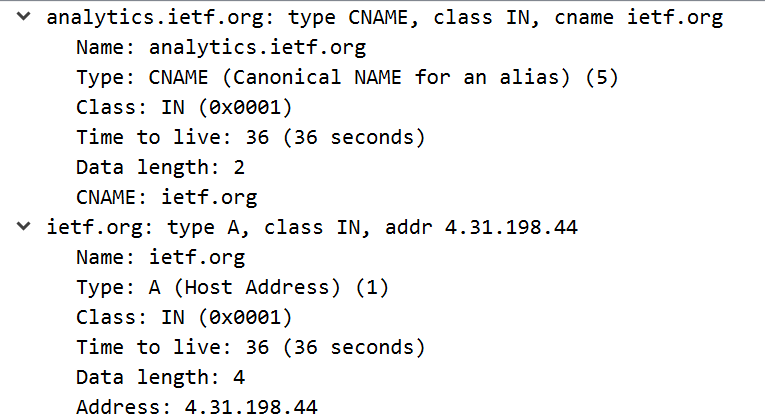
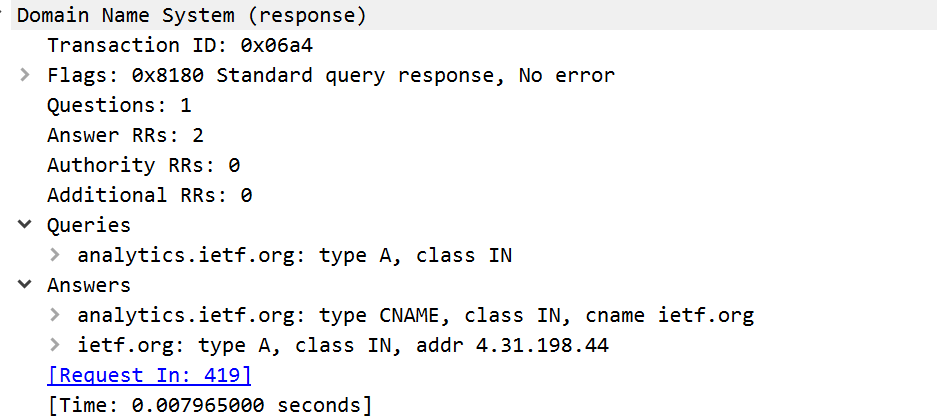


A类型；没有answers

（22）检查DNS 查询响应报文，其中提供了多少个“answers”？每个answers 包含哪些内

容？

2个；



(Name, Type, Class, TTL)另外还有 Data length和具体给出的Value。

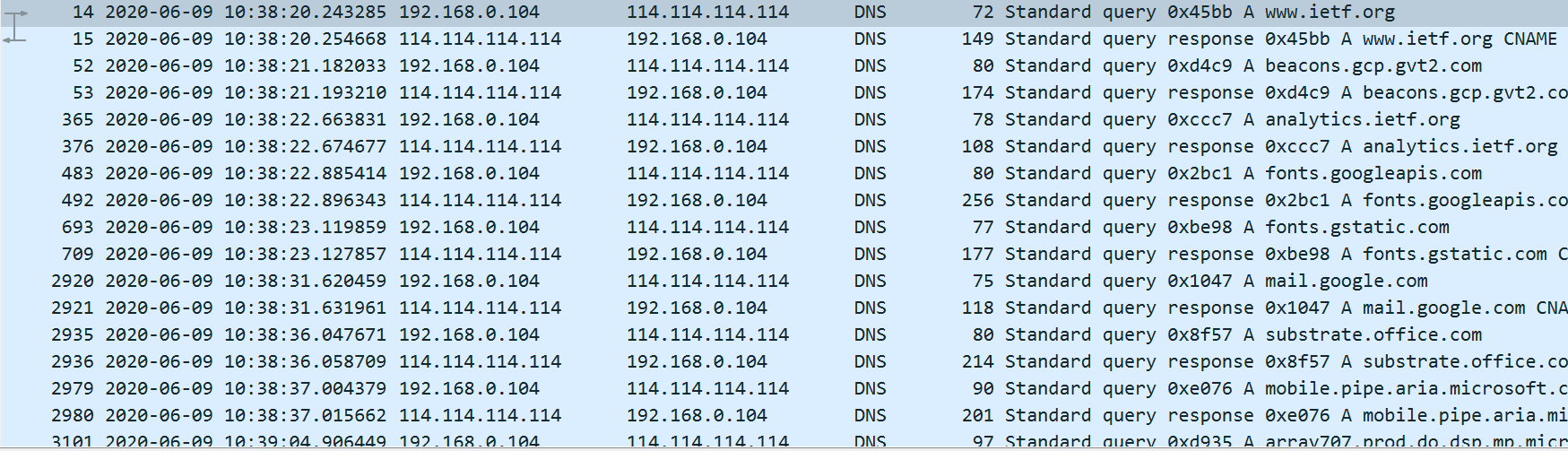
（23）考虑一下你的主机发送的并发TCP SYN 分组， SYN 分组的目的IP 地址是否与在DNS

查询响应报文中提供的某个IP 地址相对应？

是对应的。

（24）打开的WEB 页中包含图片，在获取每一个图片之前，你的主机发出新的DNS 查询了吗？

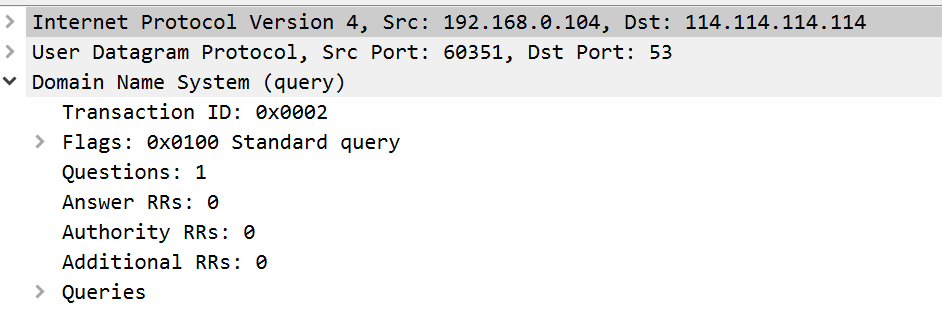
是的

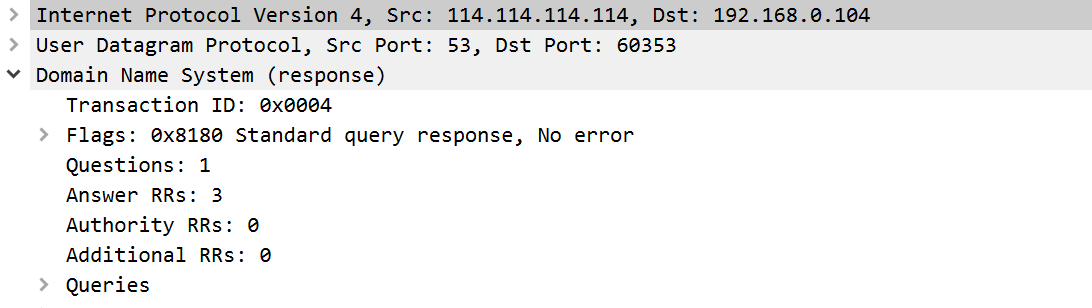


----------------------------------------------------------------------------

（25）DNS 查询报文的目的端口号是多少？DNS 查询响应报文的源端口号是多少？

53；53



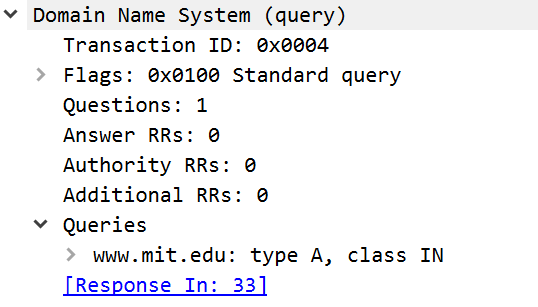


（26）DNS 查询报文发送的目的地的IP 地址是多少？这个地址是你的默认本地DNS 服务器的地址吗？

114.114.114.114； 是的

（27）检查DNS 查询报文，它是哪一类型的DNS 查询？该查询报文中包含“answers”吗？

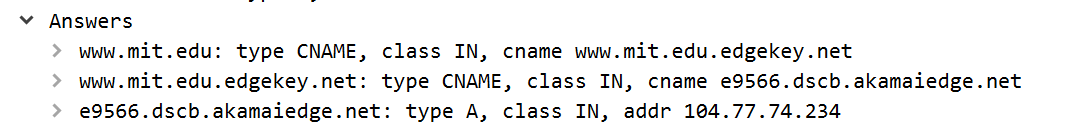
A类型；不包含answers



（28）检查DNS 查询响应报文，其中提供了多少个“answers”？每个answers 包含哪些内

容？

3个answers；



-------------------------------------------------------------------------

（29）DNS 查询报文发送的目的地的IP 地址是多少？这个地址是你的默认本地DNS 服务器的地址吗？

114.114.114.114； 是的

（30）检查DNS 查询报文，它是哪一类型的DNS 查询？该查询报文中包含“answers”吗？

NS类型；不包含

-------------------------------------------------------------------------

（32）DNS 查询报文发送的目的地的IP 地址是多少？这个地址是你的默认本地DNS 服务器的地址吗？如果不是，这个IP 地址相当于什么？

18.0.72.3；不是；这个ip是mit的权威域名服务器的。

（33）检查DNS 查询报文，它是哪一类型的DNS 查询？该查询报文中包含“answers”吗？

A类型，AAAA类型（适用于ipv6），PTR类型；没有answers

（34）检查DNS 查询响应报文，其中提供了多少个“answers”？每个answers 包含哪些内

容？

A类型的回答，对应一个answer

