WireShark 抓包实验

一. 抓包结果

整个实验共抓包两次：

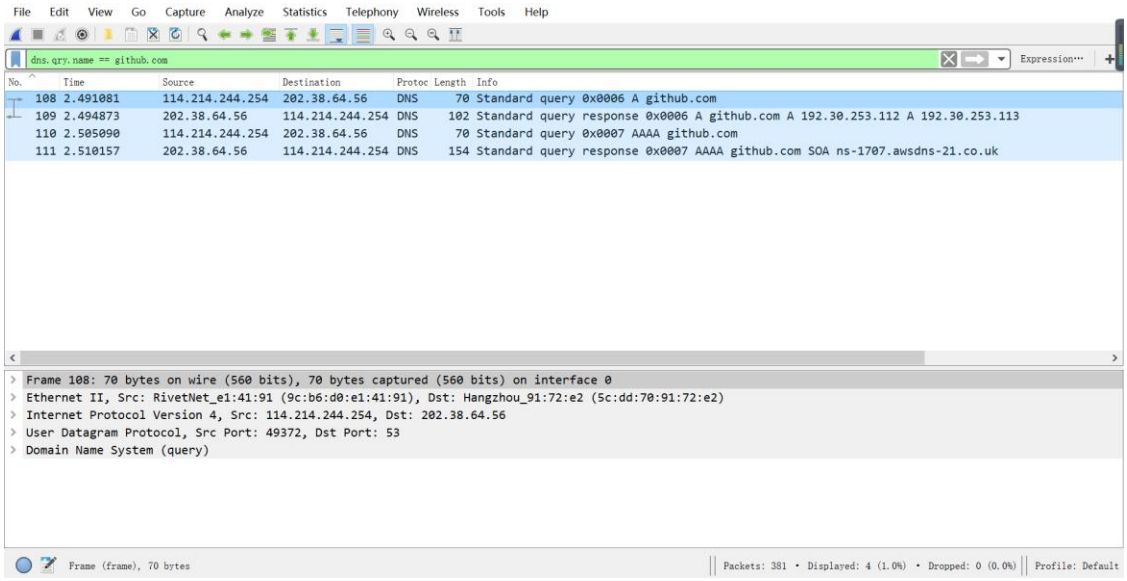
1.观察 DNS 解析过程：使用 nslookup 命令进行 DNS 查询，整个过程中用 wireshark 抓包，抓包结果保存为"学号+姓名+wireshark+1.1+cap.pcap"文件；

2.分析 https 握手过程：在浏览器中打开 https://www.github.com，整个过程用 wireshark 抓包，抓包结果保存为"学号+姓名+wireshark+1.2+cap.pcap"文件；

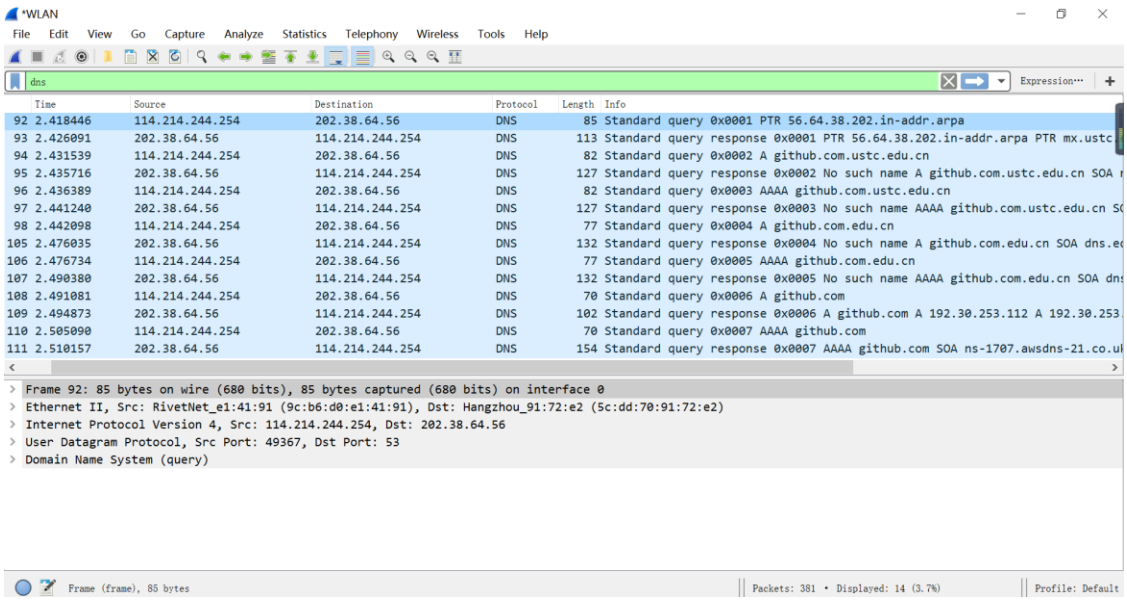
二.分析 DNS 解析过程

1.显示过滤器截图

显示过滤器：dns.qry.name==github.com



显示过滤器：dns



2.对每个数据包的解释

No.	解释
92	查询“56.64.38.202.in-addr.arpa”的域名
93	回复“92”的查询，回复内容为“mx.ustc.edu.cn”
94	查询“github.com.ustc.edu.cn”的 IPv4 地址
95	回复“94”的查询，回复内容为“No such name”
96	查询“github.com.ustc.edu.cn”的 IPv6 地址
97	回复“96”的查询，回复内容为“No such name”
98	查询“github.com.edu.cn”的 IPv4 地址
105	回复“98”的查询，回复内容为“No such name”
106	查询“github.com.edu.cn”的 IPv6 地址
107	回复“106”的查询，回复内容为“No such name”
108	查询“github.com”的 IPv4 地址
109	回复“108”的查询，回复内容为“192.30.253.112”
110	查询“github.com”的 IPv6 地址
111	回复“110”的查询，回复内容为“No such name”

3.多次出现 DNS query 的原因

可能原因 1：在 PC 使用 Nslookup 工具进行域名查询测试时，如果该 PC 是活动目录中的一台主机，默认情况下该主机除了向 DNS 服务器递交真正需要查询的域名

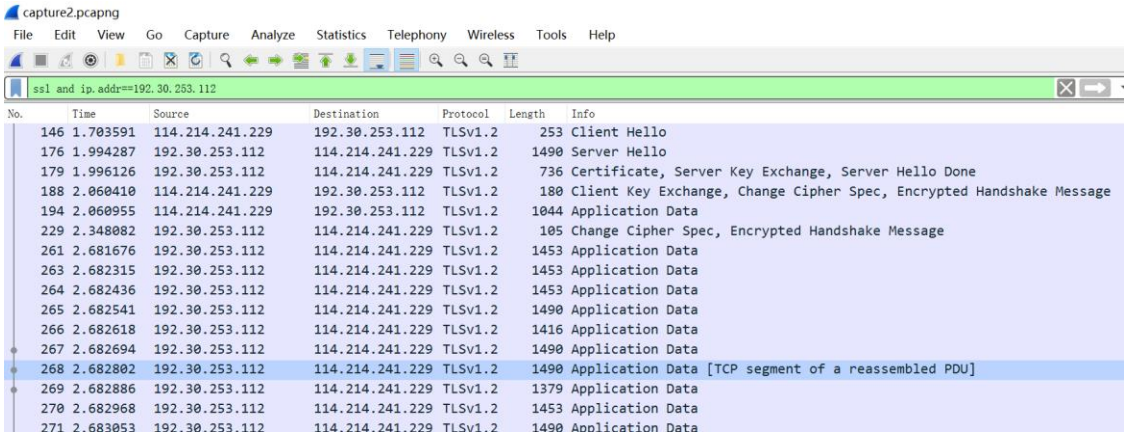
外，它还向 DNS 服务器递交“查询的域名＋活动目录域后缀”（可能为多个）这样的请求

可能原因 2：主机向本地 DNS 服务器提出请求，若本地 DNS 服务器无该域名的缓存，则本地服务器会迭代访问，过中发出多次 query

三.分析 https 握手过程

1.显示过滤器截图

显示过滤器: ssl and ip.addr == 192.30.253.112



2.握手过程分析

HTTPS 并非是应用层的一种新协议。只是 HTTP 通信接口部分用 SSL（SecureSocket Layer）和 TLS（Transport Layer Security）协议代替而已。

通常，HTTP 直接和 TCP 通信。当使用 SSL 时，则演变成先和 SSL 通信，再由 SSL 和 TCP 通信了。简言之，所谓 HTTPS，其实就是身披 SSL 协议这层外壳的 HTTP

HTTPS 共 4 次握手

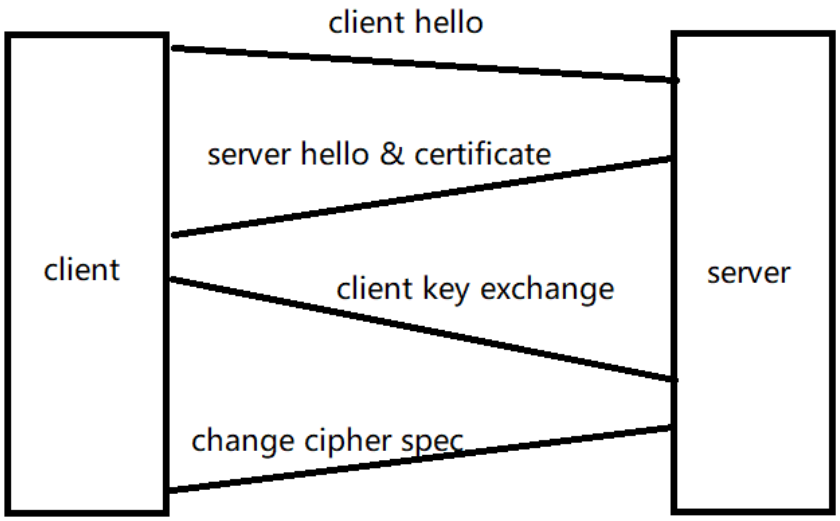
1.client to server： 客户端通过发送 Client Hello 报文开始 SSL 通信。报文中包含客户端支持的 SSL 的指定版本、加密组件（Cipher Suite）列表（所使用的*加密算法及密钥长度*等）。

2.server to client:服务器可进行 SSL 通信时，会以 Server Hello 报文作为应答。和客户端一样，在报文中包含 SSL 版本以及加密组件。服务器的加密组件内容是从接收到的客户端加密组件内筛选出来的。之后服务器发送 Certificate 报文。报文中包含*公开密钥证书*。最后服务器发送 Server Hello Done 报文通知客户端，最初阶段的 *SSL 握手协商*部分结束。

3.client to server： SSL 第一次握手结束之后，客户端以 Client Key Exchange 报文作为回应。报文中包含通信加密中使用的一种被称为 Pre-master secret 的随机密码串。该报文已用步骤 3 中的公开密钥进行加密。接着客户端继续发送 Change Cipher Spec 报文。该报文会提示服务器，在此报文之后的通信会采用 Pre-master secret 密钥加密。 客户端发送 Finished 报文。该报文包含连接至今全部报文的整体校验值。这次握手协商是否能够成功，要以服务器是否能够正确解密该报文作为判定标准

4.server to client: 服务器同样发送 Change Cipher Spec 报文。服务器同样发送 Finished 报文。

3.握手过程交互图



4.每次交互对应的数据包 No.

第 1 次：No.146

第 2 次：No.176 , No.179

第 3 次：No.188 , No.194

第 4 次：No.229