使用 Wireshark 追踪 DNS 数据包

首先，让我们捕获由一般情况下用浏览器访问域名时生成的 DNS 数据包。步骤如下：

- 清空本机 DNS 缓存。(使用 ipconfig/flushdns 指令)
- 浏览器缓存。(如 Chrome 浏览器：地址栏输入 chrome://net-internals/#dns 后点击“clear host cache”)
- 设置 Wireshark 的显示过滤器为 DNS，并选择当前连接的网络。
- 点击开始捕获分组按钮。
- 打开浏览器访问任意一个网站。（例如 http://www. bilibili.com）
- 等待网页加载完毕后点击停止捕获分组按钮。
- 分析 DNS 数据包，回答下面的 5 题：

1. 找到 www.bilibili.com 的 DNS 查询（query）和响应(response)报文。 它们是通过 UDP 还是 TCP 发送的?
2. 该 DNS 查询报文的目标端口（destination port）是什么？DNS 响应报文的源端口（source port）是什么？请回答+截图框选相应信息。
3. 该 DNS 查询报文发送到哪个 IP 地址？ 是你的默认本地 DNS 服务器的 IP 地址吗？（使用 ipconfig/all 查看本地 DNS 服务器的 IP 地址。如果是多个，默认第一个）请回答+截图框选相应信息。
4. 该 DNS 查询报文的“Type”是什么？ 查询报文是否包含任何“answers”？请回答+截图框选相应信息。
5. 该 DNS 响应报文提供了多少个“answers”？请回答+截图框选相应信息。

现在我们分析 nslookup 指令所产生的 DNS 数据包。步骤如下：

- 设置 Wireshark 的显示过滤器为 DNS，并选择当前连接的网络。
- 点击开始捕获分组按钮。
- 在命令行中输入：nslookup www.fudan.edu.cn
- 等待指令完成后点击停止捕获分组按钮。
- 分析 DNS 数据包，回答下面的 5 题：

6. 找到 www.fudan.edu.cn 的 DNS 查询（query）和响应(response)报文。 它们是通过 UDP 还是 TCP 发送的?
7. 该 DNS 查询报文的目标端口（destination port）是什么？DNS 响应报文的源端口（source port）是什么？请回答+截图框选相应信息。
8. 该 DNS 查询报文发送到哪个 IP 地址？是你的默认本地 DNS 服务器的 IP 地址吗？请回答+截图框选相应信息。
9. 该 DNS 查询报文的“Type”是什么？ 查询报文是否包含任何“answers”？请回答+截图框选相应信息。
10. 该 DNS 响应报文提供了多少个“answers”？请回答+截图框选相应信息。

现在我们重复上面的步骤，只是将命令行指令换为：
`nslookup -type=NS fudan.edu.cn`
然后回答下面的 3 题：

11. 该 DNS 查询报文发送到哪个 IP 地址？是你的默认本地 DNS 服务器的 IP 地址吗？请回答+截图框选相应信息。
12. 该 DNS 查询报文的“Type”是什么？ 查询报文是否包含任何“answers”？请回答+截图框选相应信息。
13. 该 DNS 响应报文提供了哪些复旦名称服务器（Name Server）？该响应消息是否也提供复旦名称服务器的 IP 地址？

现在我们重复上面的步骤，只是将命令行指令换为：
`nslookup www.fudan.edu.cn public1.alidns.com`
然后回答下面的 3 题：

14. 该 DNS 查询报文发送到哪个 IP 地址？是你的默认本地 DNS 服务器的 IP 地址吗？如果不是，该 IP 地址对应什么？请回答+截图框选相应信息。
15. 该 DNS 查询报文的“Type”是什么？ 查询报文是否包含任何“answers”？请回答+截图框选相应信息。
16. 该 DNS 响应报文提供了多少个“answers”？请回答+截图框选相应信息。