

实验 - 了解 DNS 流量

目标

第 1 部分：捕获 DNS 流量

第 2 部分：了解 DNS 查询流量

第 3 部分：了解 DNS 响应流量

背景/场景

Wireshark 是一款开源式数据包捕获和分析工具。Wireshark 能够显示网络协议栈的详细内容。Wireshark 允许同学们过滤流量，从而进行网络故障排除，调查安全问题和分析网络协议。因为 Wireshark 允许同学们查看数据包详细信息，所以它可以用作攻击者的侦查跟踪工具。

在本实验中，同学们将在 Windows 系统上安装 Wireshark，并使用 Wireshark 来过滤 DNS 数据包，并查看 DNS 查询和响应数据包的详细信息。

所需资源

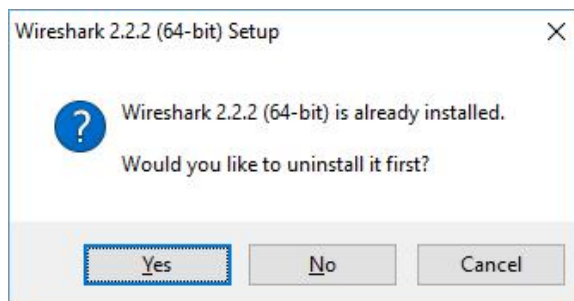
- 1 台接入互联网并安装了 Wireshark 的 Windows PC

第 1 部分： 捕获 DNS 流量

第 1 步： 下载并安装 Wireshark。

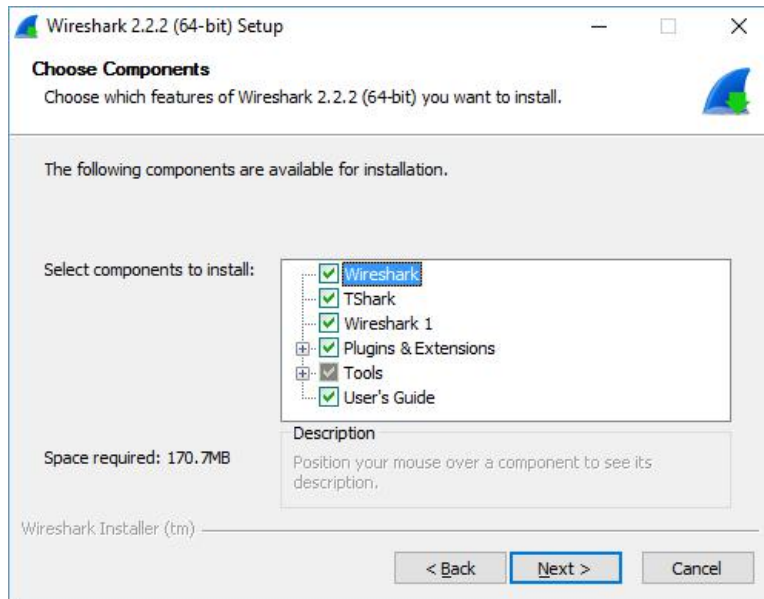
- 为 Windows 安装 Wireshark。
- Wireshark 可从 www.wireshark.org 下载。
- 根据 PC 架构和操作系统选择所需的软件版本。例如，如果使用运行 Windows 的 64 位 PC，则选择“**Windows Installer (64 位)**”。
- 选择后，下载应该就会开始。已下载文件的位置取决于同学们所使用的浏览器和操作系统。对于 Windows 用户，默认位置是“**下载**”文件夹。
- 下载的文件命名为 **Wireshark-win64-x.x.x.exe**，其中 **x** 代表版本号。双击文件开始安装过程。

对屏幕上可能显示的任何安全消息做出响应。如果 PC 上已经有一个 Wireshark 的副本，则系统会提示卸载旧版本，然后安装新版本。建议同学们在安装另一版本之前先删除旧的 Wireshark 版本。点击“**是**”卸载之前的 Wireshark 版本。



- 如果是第一次安装 Wireshark，或者在完成卸载过程后，同学们将导航至 Wireshark 安装向导。点击**下一步**。

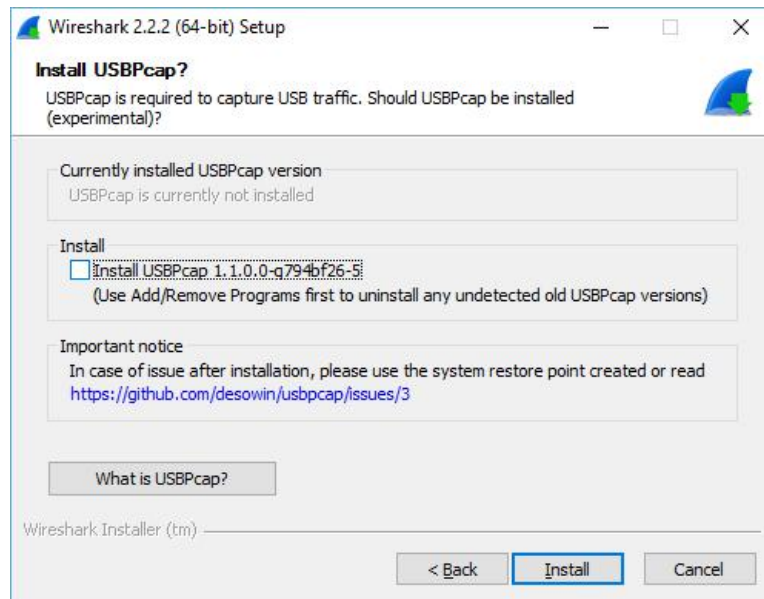
- g. 继续完成安装过程。当显示“许可协议”窗口时，点击“我同意”。
- h. 保持“选择组件”窗口的默认设置，并点击“下一步”。



- i. 选择所需的快捷选项，然后点击“下一步”。
- j. 同学们可以更改 Wireshark 的安装位置，但是除非磁盘空间有限，否则建议同学们保持默认位置。点击下一步继续。
- k. 要捕获实时网络数据，必须在 PC 上安装 WinPcap。如果同学们的 PC 上已经安装了 WinPcap，则“安装”复选框会处于取消选中状态。如果同学们之前安装的 WinPcap 比 Wireshark 附带的版本旧，建议同学们点击“安装 WinPcap x.x.x (版本号)”复选框以允许安装较新版本。

如果安装 WinPcap，请完成 WinPcap 安装向导，并在必要时接受许可协议。点击下一步继续。

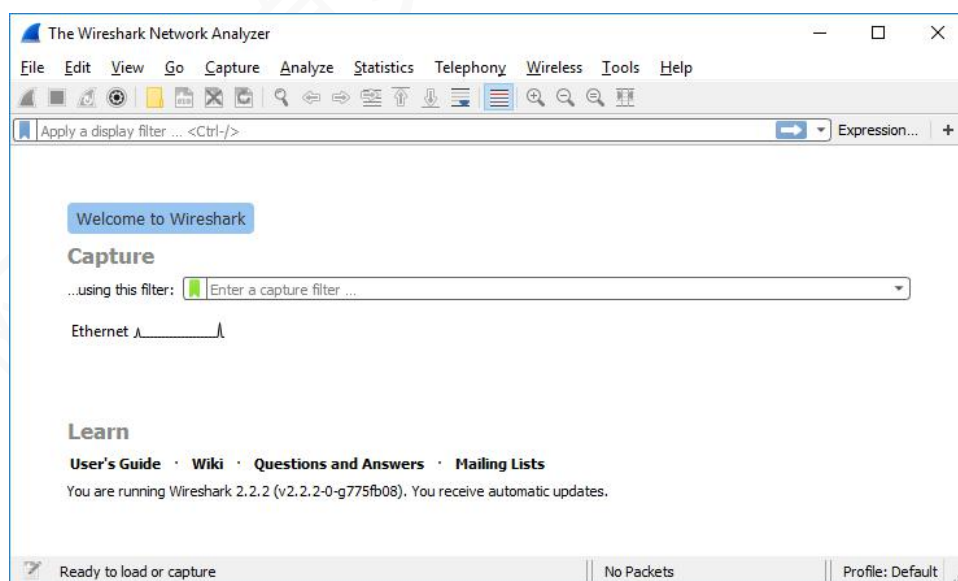
- l. 请勿安装用于捕获正常流量的 USBPcap。请勿选中安装 **USBPcap** 的复选框。USBPcap 是实验性产品，它可能会导致同学们的 PC 出现 USB 问题。点击**安装继续**。



- m. Wireshark 开始安装其文件，而且会出现一个独立窗口，显示安装状态。安装完成后，点击“**下一步**”。
- n. 点击“**完成**”完成 Wireshark 安装过程。如有必要，重新启动计算机。

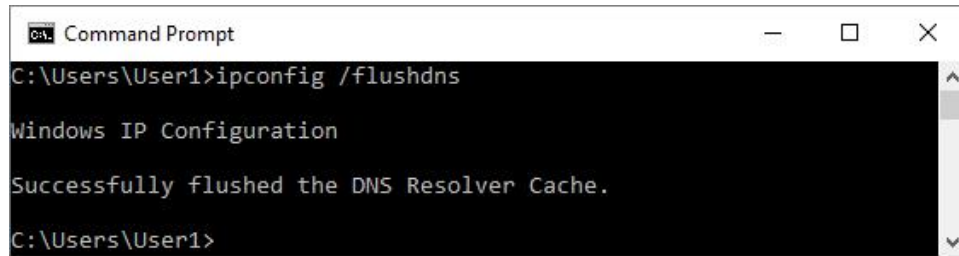
第 2 步： 捕获 DNS 流量。

- a. 点击**开始并搜索 Wireshark**。打开 **Wireshark** 并通过双击有流量的网络接口来开始 Wireshark 捕获。在本例中，以太网是有流量的网络接口。



- b. 点击**开始并搜索命令提示符**。打开**命令提示符**。

- c. 在命令提示符后，键入 **ipconfig /flushdns** 并按 Enter 键清除 DNS 缓存。



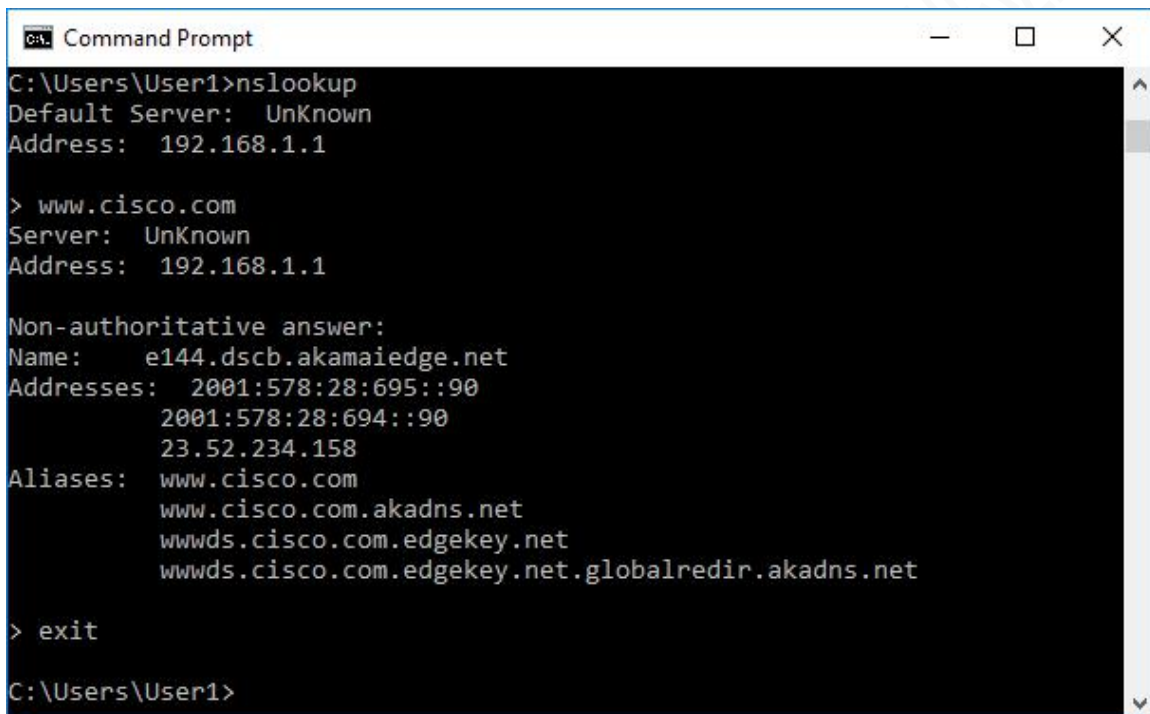
```
Command Prompt
C:\Users\User1>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\User1>
```

- d. 键入 **nslookup**，然后按 Enter 键进入交互模式。
- e. 输入网站的域名。本例中使用的域名为 www.cisco.com。



```
Command Prompt
C:\Users\User1>nslookup
Default Server: UnKnown
Address: 192.168.1.1

> www.cisco.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: e144.dscb.akamaiedge.net
Addresses: 2001:578:28:695::90
           2001:578:28:694::90
           23.52.234.158
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net

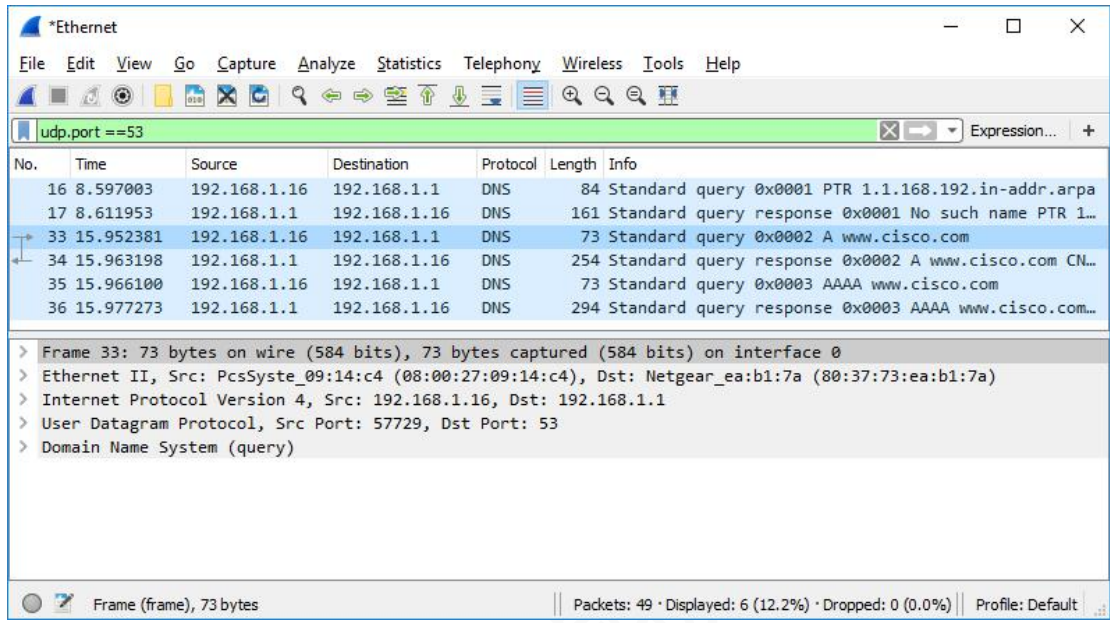
> exit

C:\Users\User1>
```

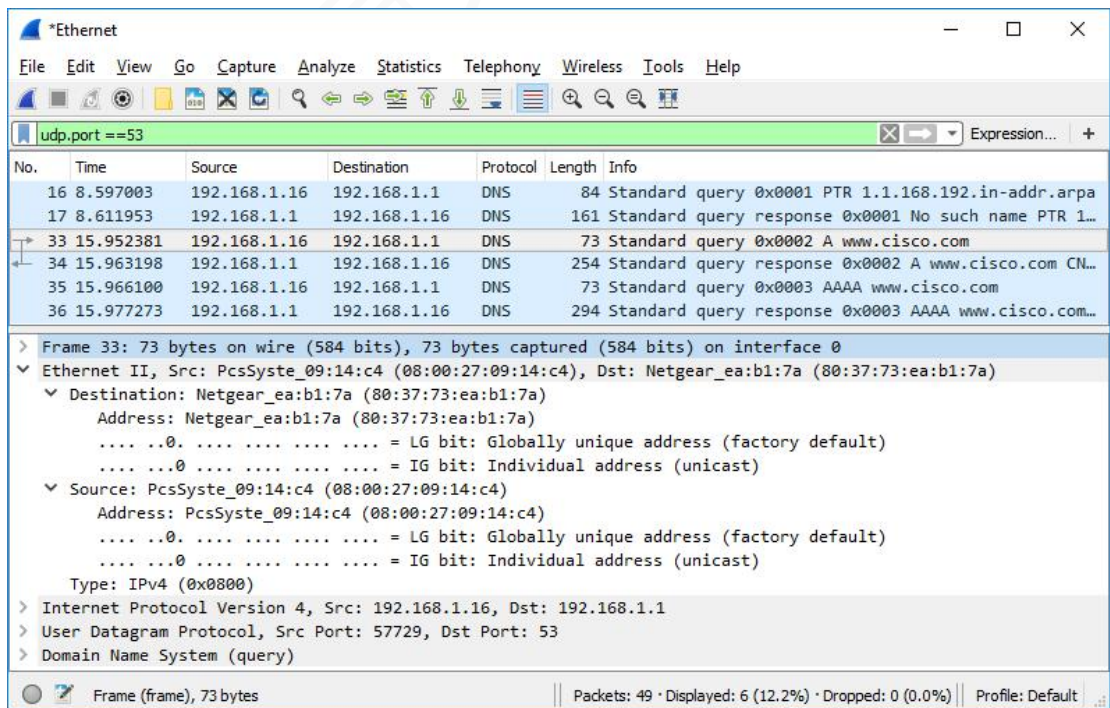
- f. 完成后键入 **exit**。关闭命令提示符。
- g. 点击**停止捕获数据包**以停止 Wireshark 捕获。

第 2 部分： 了解 DNS 查询流量

- a. 观察在“Wireshark 数据包列表”窗格中捕获的流量。在过滤器方框中输入 `udp.port == 53`，然后点击箭头（或按 Enter 键）只显示 DNS 数据包。

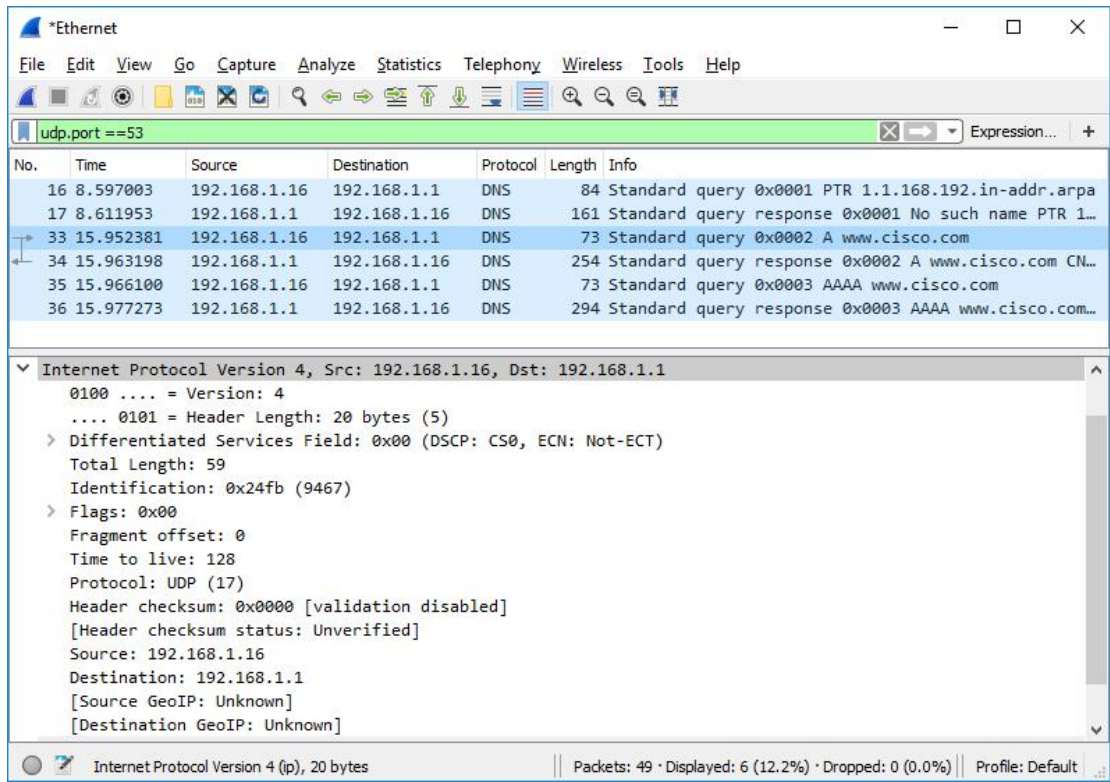


- b. 选择标记为 **Standard query 0x0002 A www.cisco.com** 的 DNS 数据包。
- c. 在“数据包详细信息”窗格中，请注意此数据包具有以太网 II、互联网协议第四版、用户数据报协议和域名系统（查询）。
- d. 展开以太网 II 以查看详细信息。观察源和目的字段。



源和目的 MAC 地址是什么？这些 MAC 地址与哪些网络接口相关联？

e. 展开互联网协议第四版。观察源和目的 IPv4 地址。



源和目的 IP 地址是什么？这些 IP 地址与哪些网络接口相关联？

f. 展开用户数据报协议。观察源和目的端口。

Wireshark packet capture window titled "Ethernet". The filter bar shows "udp.port == 53". The packet list shows several DNS packets. Packet 33 is selected, showing details for User Datagram Protocol (UDP) and Domain Name System (query). The UDP section shows Source Port: 57729 and Destination Port: 53. The DNS section shows a query for "PTR 1.1.168.192.in-addr.arpa".

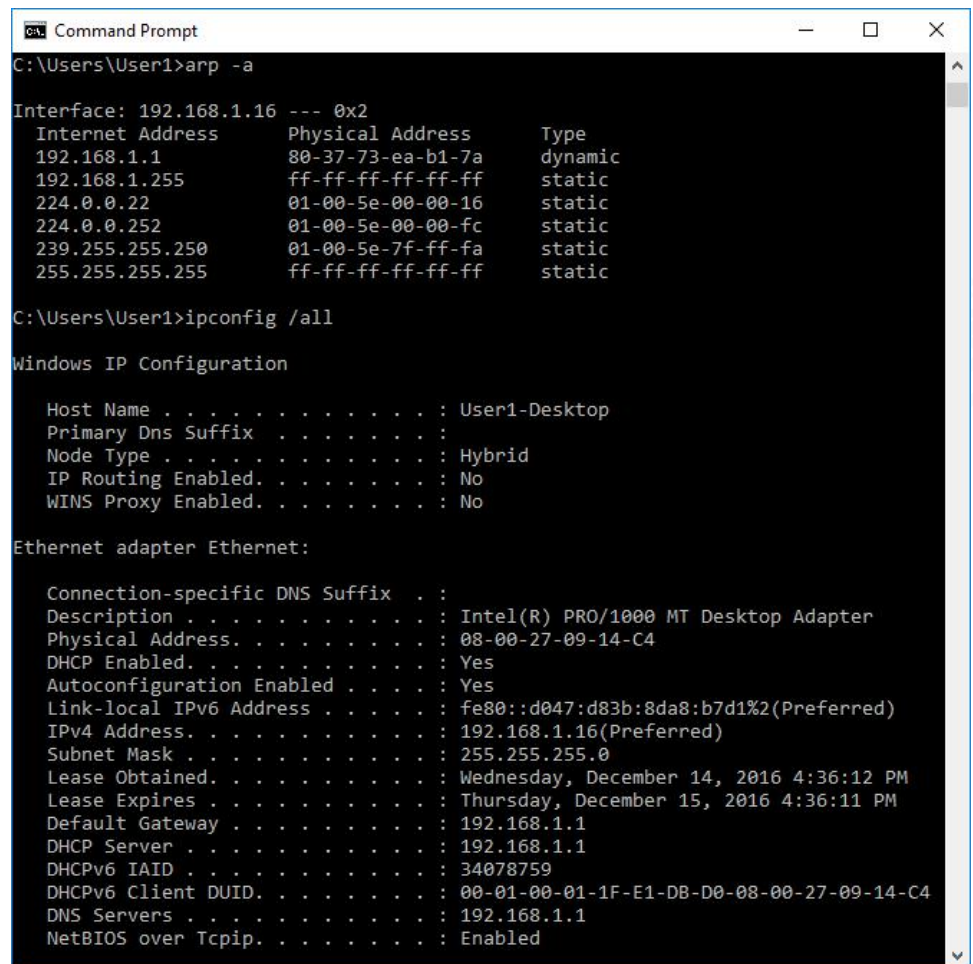
No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 57729, Dst Port: 53
Source Port: 57729
Destination Port: 53
Length: 39
Checksum: 0x839a [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
> Domain Name System (query)

User Datagram Protocol (udp), 8 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

源和目的端口是什么？默认 DNS 端口号是什么？

- g. 打开命令提示符并输入 **arp -a** 和 **ipconfig /all** 以记录 PC 的 MAC 和 IP 地址。



```
Command Prompt
C:\Users\User1>arp -a

Interface: 192.168.1.16 --- 0x2
   Internet Address      Physical Address        Type
   -----
   192.168.1.1            80-37-73-ea-b1-7a      dynamic
   192.168.1.255          ff-ff-ff-ff-ff-ff      static
   224.0.0.22             01-00-5e-00-00-16      static
   224.0.0.252            01-00-5e-00-00-fc      static
   239.255.255.250        01-00-5e-7f-ff-fa      static
   255.255.255.255        ff-ff-ff-ff-ff-ff      static

C:\Users\User1>ipconfig /all

Windows IP Configuration

   Host Name . . . . . : User1-Desktop
   Primary Dns Suffix . . . . . :
   Node Type . . . . . : Hybrid
   IP Routing Enabled. . . . . : No
   WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . : 08-00-27-09-14-C4
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d047:d83b:8da8:b7d1%2(Preferred)
   IPv4 Address. . . . . : 192.168.1.16(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Lease Obtained. . . . . : Wednesday, December 14, 2016 4:36:12 PM
   Lease Expires . . . . . : Thursday, December 15, 2016 4:36:11 PM
   Default Gateway . . . . . : 192.168.1.1
   DHCP Server . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . : 34078759
   DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-E1-DB-D0-08-00-27-09-14-C4
   DNS Servers . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . : Enabled
```

将 Wireshark 结果中的 MAC 和 IP 地址与 **ipconfig /all** 结果进行比较。同学们观察出了什么？

- h. 展开“数据包详细信息”窗格中的**域名系统（查询）**。然后，展开**标志**和**查询**。

- i. 观察结果。该标志设置为以递归方式执行查询，以查询 `www.cisco.com` 的 IP 地址。

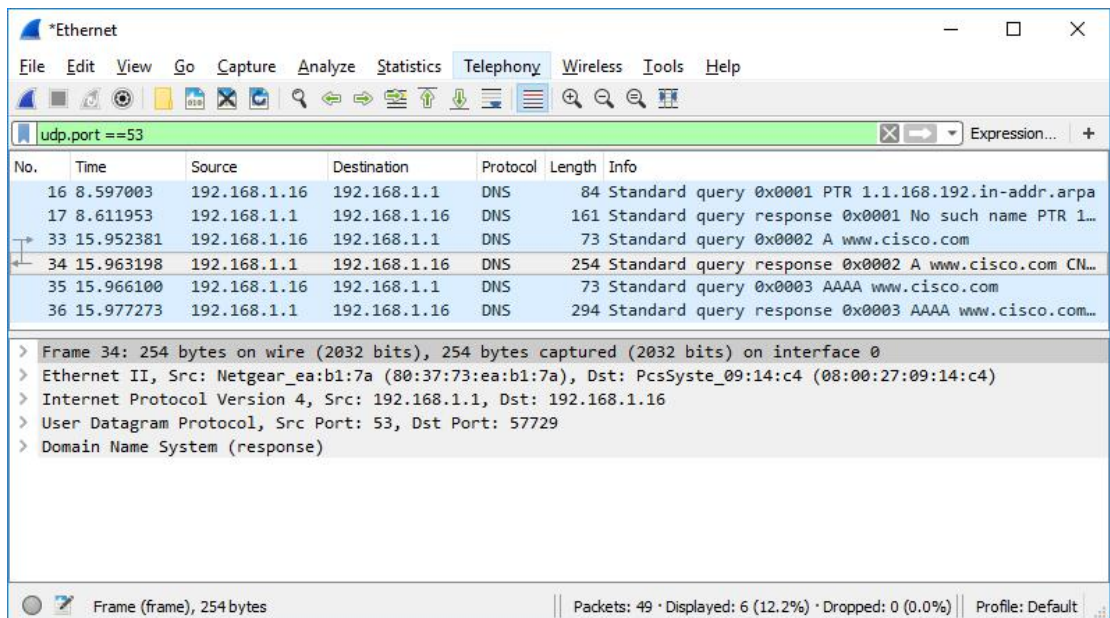
The screenshot shows a Wireshark packet capture window titled "Ethernet". The filter bar at the top contains the expression `udp.port == 53`. The packet list shows several DNS packets. Packet 34 is selected, and its details pane is expanded to show the "Domain Name System (query)" section. The details pane shows the following information:

- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 57729, Dst Port: 53
- Domain Name System (query)
 - [Response In: 34]
 - Transaction ID: 0x0002
 - Flags: 0x0100 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)
 -0... .. = Non-authenticated data: Unacceptable
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.cisco.com: type A, class IN
 - Name: www.cisco.com
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

The status bar at the bottom indicates "Domain Name System (dns), 31 bytes" and "Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)".

第 3 部分： 了解 DNS 响应流量

- a. 选择标记为 **Standard query response 0x000# A www.cisco.com** 的相应的响应 DNS 数据包。



The screenshot shows the Wireshark network protocol analyzer interface. The packet list pane displays several captured packets, with packet 34 selected. The packet details pane shows the structure of the selected packet, which is a DNS response. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

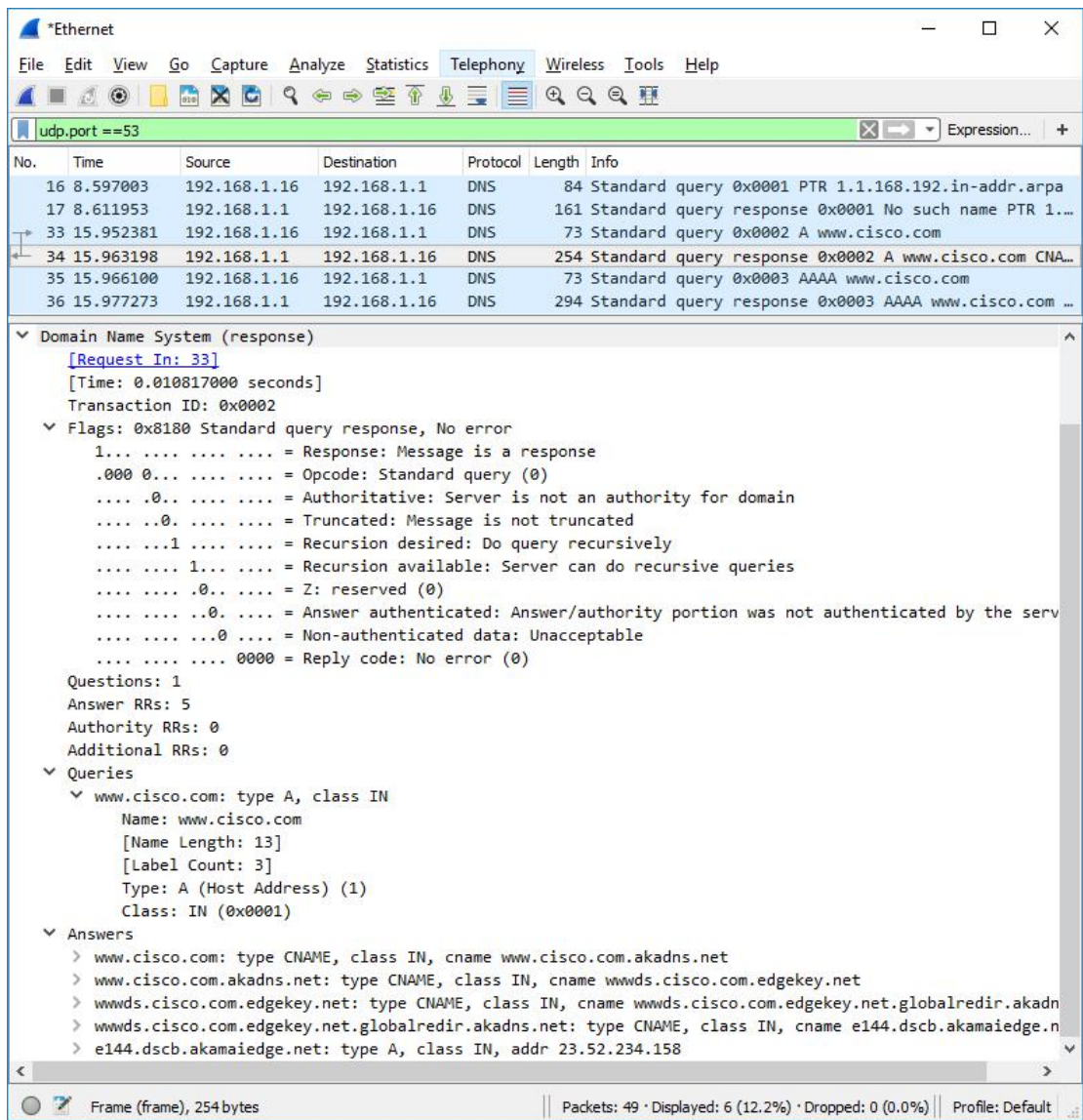
The packet details pane for packet 34 shows the following structure:

- > Frame 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
- > Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: Pcsyste_09:14:c4 (08:00:27:09:14:c4)
- > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
- > User Datagram Protocol, Src Port: 53, Dst Port: 57729
- > Domain Name System (response)

源和目的 MAC 和 IP 地址以及端口号是什么？它们如何与 DNS 查询数据包中的地址进行比较？

- b. 展开域名系统（响应）。然后，展开标志、查询和应答。

c. 观察结果。DNS 服务器是否可以执行递归查询？ _____



d. 观察“应答”详细信息中的 CNAME 和 A 记录。这些结果如何与 nslookup 结果进行比较？ _____

思考

1. 在 Wireshark 结果中，当同学们删除过滤器时，还能了解到网络的哪些其他信息？

2. 攻击者如何使用 Wireshark 来破坏同学们的网络安全？

