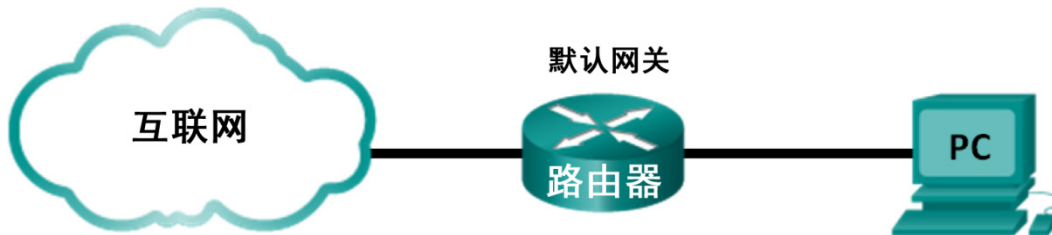


实验 - 使用 Wireshark 观察 TCP 三次握手

拓扑



目标

第 1 部分：准备 Wireshark 以捕获数据包

第 2 部分：捕获、定位和检查数据包

背景/场景

在本实验中，您将使用 Wireshark 来捕获并检查数据包，数据包是在使用超文本传输协议 (HTTP) 的 PC 浏览器和 Web 服务器（例如 www.google.com）之间生成的。当一个应用程序，例如 HTTP 或文件传输协议 (FTP)，在主机上首次启动时，TCP 将使用三次握手来建立两个主机之间的可靠 TCP 会话。例如，当 PC 使用 Web 浏览器浏览互联网时，将会发起三次握手，而且 PC 主机和 Web 服务器之间将建立会话。一个 PC 可以同时与多个网站进行多个活动的 TCP 会话。

注意：此实验不能使用 Netlab 完成。此实验假设您具有互联网访问。

所需资源

1 台 PC（采用 Windows 7 或 8 且可访问命令提示符、互联网，并且已安装 Wireshark）

第 1 部分：准备 Wireshark 以捕获数据包

在第 1 部分中，您将启动 Wireshark 程序并选择适当的接口开始捕获数据包。

第 1 步：检索 PC 的接口地址。

对于本实验，您需要检索 PC 的 IP 地址及其网络接口卡 (NIC) 物理地址（也称为 MAC 地址）。

a. 打开命令提示符窗口，键入 `ipconfig /all`，然后按 Enter 键。

```

Physical Address. . . . . : 00-1A-73-EA-63-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%14(Preferred)
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
  
```

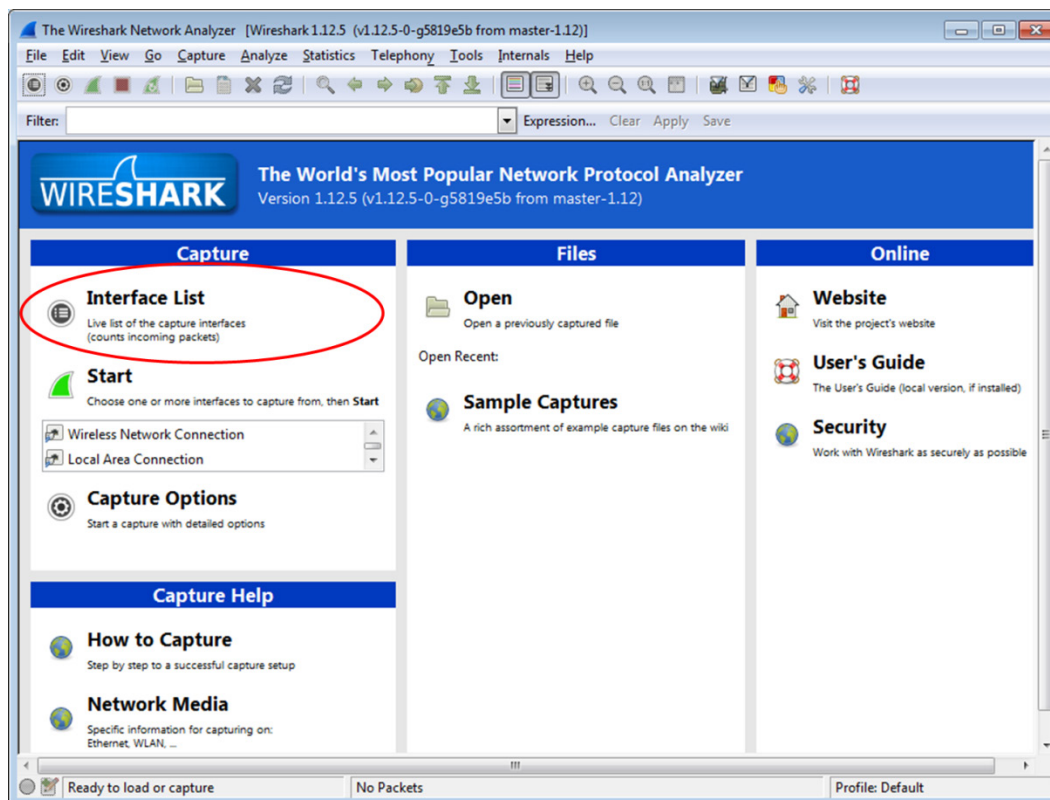
b. 写下与选定的以太网适配器相关联的 IP 地址和 MAC 地址。检查捕获的数据包时，这是源地址。

PC 的主机 IP 地址： _____

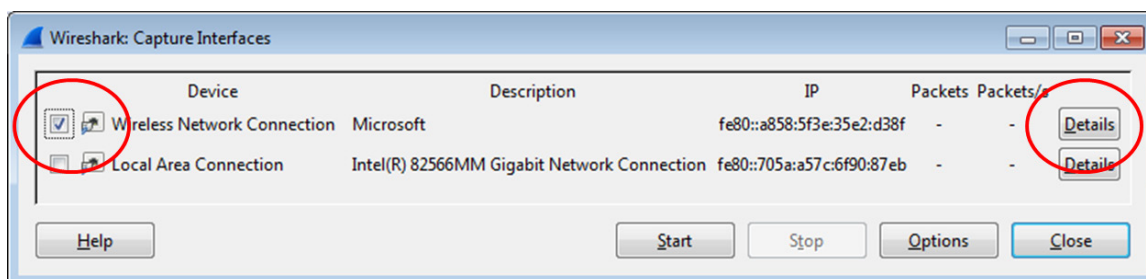
PC 的主机 MAC 地址： _____

第 2 步：启动 Wireshark 并选择适当的接口。

- 单击 Windows **Start**（开始）按钮。在弹出菜单中双击 **Wireshark**。
- 在 Wireshark 启动之后，单击 **Interface List**（接口列表）。



- 在 **Wireshark: Capture Interfaces**（Wireshark：捕获接口）窗口中，单击与您的 LAN 连接的接口旁的复选框。



注意：如果列出了多个接口，而您不能确定要选择哪个接口，请单击 **Details**（详细信息）。单击 **802.3 (Ethernet)** [802.3 (以太网)] 选项卡，并验证 MAC 地址是否与您在步骤 1b 中记录的相匹配。验证完成后关闭 Interface Details（接口详细信息）窗口。

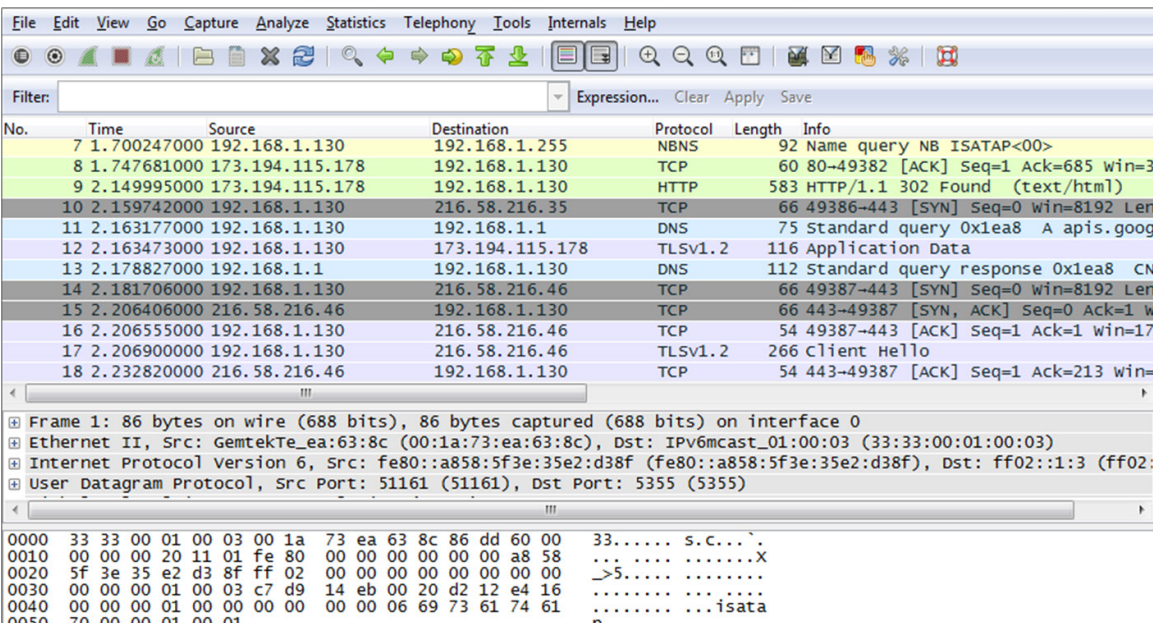
第 2 部分：捕获、定位和检查数据包

第 1 步：捕获数据。

- a. 单击 **Start**（开始）按钮开始数据捕获。
- b. 导航至 www.google.com。将浏览器最小化，返回到 Wireshark。停止数据捕获。

注意：教师可能会提供其他的网站。请在此写下网站名称或地址：

现在捕获窗口处于活动状态。找到 **Source**（源）、**Destination**（目的地）和 **Protocol**（协议）列。



No.	Time	Source	Destination	Protocol	Length	Info
7	1.700247000	192.168.1.130	192.168.1.255	NBNS	92	Name query NB ISATAP<00>
8	1.747681000	173.194.115.178	192.168.1.130	TCP	60	80->49382 [ACK] Seq=1 Ack=685 win=3
9	2.149995000	173.194.115.178	192.168.1.130	HTTP	583	HTTP/1.1 302 Found (text/html)
10	2.159742000	192.168.1.130	216.58.216.35	TCP	66	49386->443 [SYN] Seq=0 win=8192 Len=
11	2.163177000	192.168.1.130	192.168.1.1	DNS	75	Standard query 0x1ea8 A apis.goog
12	2.163473000	192.168.1.130	173.194.115.178	TLSv1.2	116	Application Data
13	2.178827000	192.168.1.1	192.168.1.130	DNS	112	Standard query response 0x1ea8 CN
14	2.181706000	192.168.1.130	216.58.216.46	TCP	66	49387->443 [SYN] Seq=0 win=8192 Len=
15	2.206406000	216.58.216.46	192.168.1.130	TCP	66	443->49387 [SYN, ACK] Seq=0 Ack=1 W
16	2.206555000	192.168.1.130	216.58.216.46	TCP	54	49387->443 [ACK] Seq=1 Ack=1 win=17
17	2.206900000	192.168.1.130	216.58.216.46	TLSv1.2	266	Client Hello
18	2.232820000	216.58.216.46	192.168.1.130	TCP	54	443->49387 [ACK] Seq=1 Ack=213 win=

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
Internet Protocol Version 6, Src: fe80::a858:5f3e:35e2:d38f (fe80::a858:5f3e:35e2:d38f), Dst: ff02::1:3 (ff02::1:3)
User Datagram Protocol, Src Port: 51161 (51161), Dst Port: 5355 (5355)

0000 33 33 00 01 00 03 00 1a 73 ea 63 8c 86 dd 60 00 33.....s.c...
0010 00 00 00 20 11 01 fe 80 00 00 00 00 00 00 a8 58 ...X
0020 5f 3e 35 e2 d3 8f ff 02 00 00 00 00 00 00 00 00 >5...
0030 00 00 00 01 00 03 c7 d9 14 eb 00 20 d2 12 e4 16
0040 00 00 01 00 00 00 00 00 00 00 06 69 73 61 74 61isata

第 2 步：查找 Web 会话的相应数据包。

如果计算机是最近启动的而且没有访问互联网，则您可以在捕获输出中看到整个过程，包括地址解析协议 (ARP)、域名系统 (DNS) 和 TCP 三次握手。如果 PC 已经拥有默认网关的 ARP 条目；因此它首先发出 DNS 查询以解析 www.google.com。

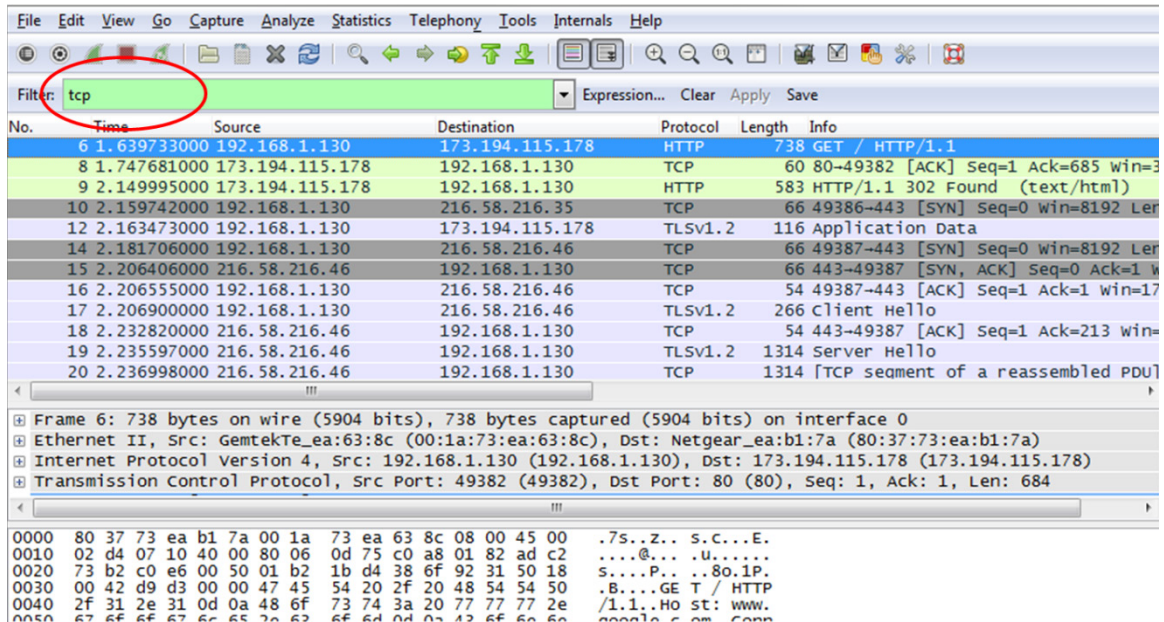
- a. 帧 11 显示了从 PC 发送到 DNS 服务器的 DNS 查询，尝试将域名 (www.google.com) 解析为 Web 服务器的 IP 地址。PC 必须获取到该 IP 地址才能将第一个数据包发送至 Web 服务器。

计算机查询的 DNS 服务器的 IP 地址是多少？ _____

- b. 帧 13 是来自 DNS 服务器的响应。它包含 www.google.com 的 IP 地址。
- c. 找到相应数据包以开始三次握手。在本例中，帧 14 是 TCP 三次握手的开始。

Google Web 服务器的 IP 地址是多少？ _____

- d. 如果您有许多与 TCP 连接无关的数据包，则可能需要使用 Wireshark 过滤器工具。在 Wireshark 的过滤器条目区域中输入 **tcp** 并按 **Enter** 键。

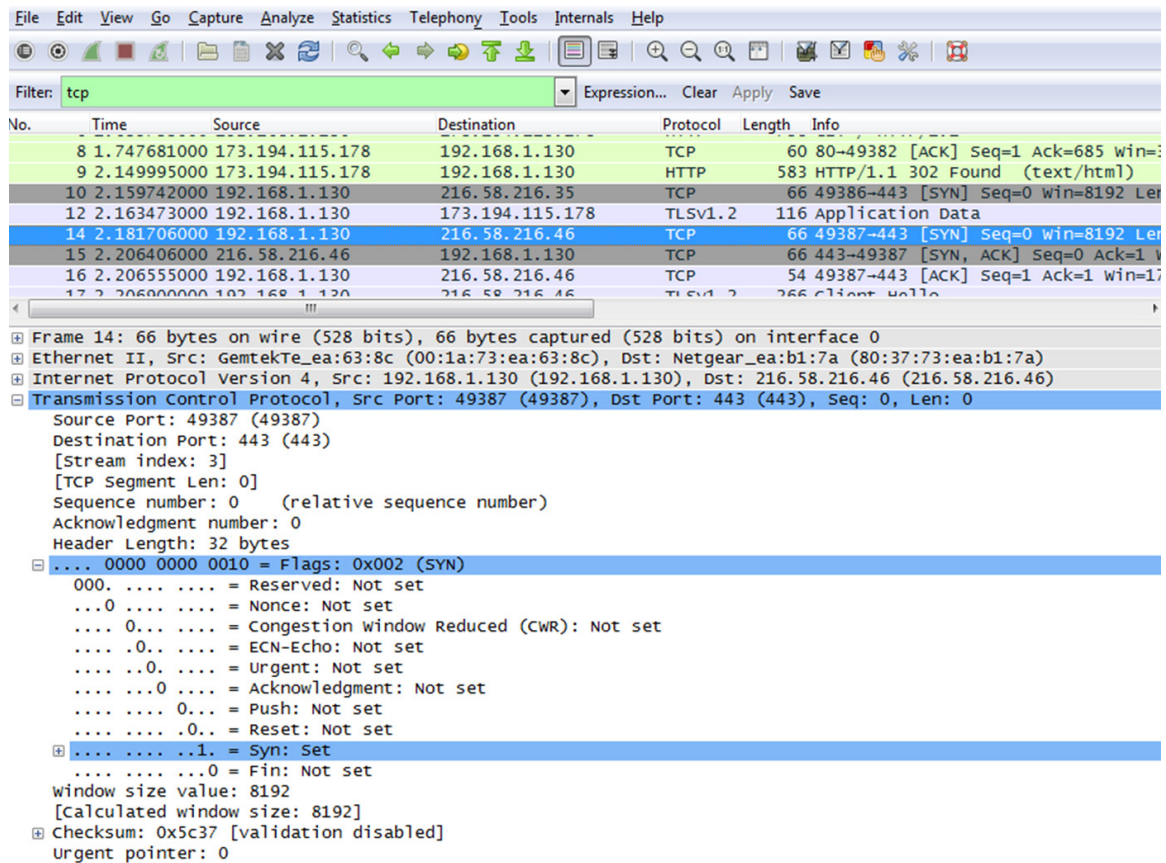


第 3 步：检查数据包中的信息，包括 IP 地址、TCP 端口号和 TCP 控制标志。

- a. 在我们的示例中，帧 14 是 PC 和 Google Web 服务器之间三次握手的开始。在数据包列表窗格（主窗口的顶部）中选择此帧。这将使这一行突出显示，并在下面两个窗格中显示该数据包的解码信息。检查数据包详细信息窗格（主窗口的中间部分）中的 TCP 信息。
- b. 单击数据包详细信息窗格中传输控制协议左侧的 + 图标展开 TCP 信息显示。

- c. 单击 Flags（标志）左侧的 + 图标。查看源端口和目的端口以及所设置的标志。

注意：您可能需要调整 Wireshark 中顶部和中间窗口的大小以显示所需信息。



TCP 的源端口号是什么？ _____

您将该源端口如何归类？ _____

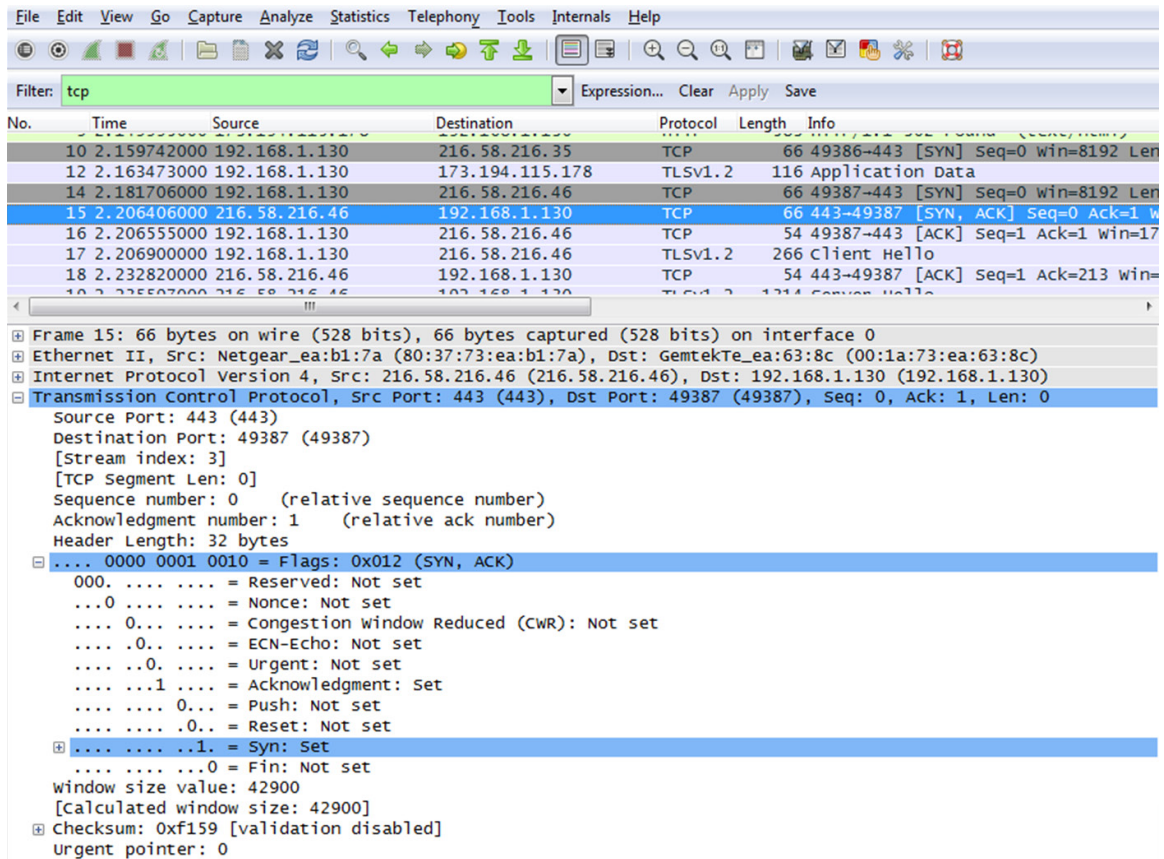
TCP 的目的端口号是什么？ _____

您将该目的端口如何归类？ _____

设置了哪些标志？ _____

相应的序列号设置为多少？ _____

- d. 要选择三次握手中的下一个帧，请在 Wireshark 菜单中选择 **Go**（转至）并选择 **Next Packet In Conversation**（对话中的下一数据包）。在本例中是帧 15。这是 Google Web 服务器对启动会话的初始请求作出的响应。

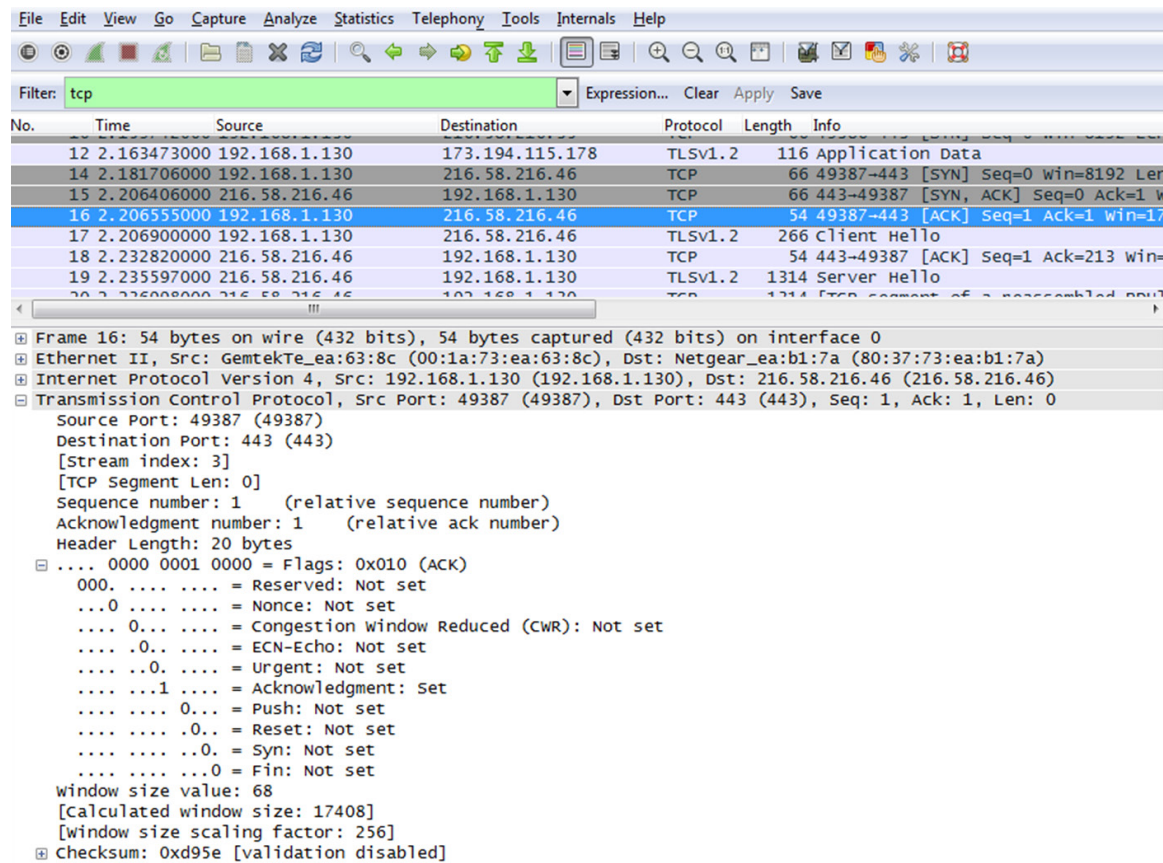


源端口和目的端口的值是什么？ _____

设置了哪些标志？ _____

相应的序列号和确认号设置为什么？ _____

e. 最后，检查示例中三次握手的第三个数据包。单击窗口顶部的帧 16 将显示本例中的以下信息：



检查握手的第三个和最后一个数据包。

设置了哪些标志？ _____

将相应的序列号和确认号设置为 1 作为起点。TCP 连接已建立，源计算机与 Web 服务器之间可以开始通信。

f. 关闭 Wireshark 程序。

思考

1. 在 Wireshark 中有上百个过滤器可用。大型网络可以有多个过滤器和许多不同类型的流量。请列出可能对网络管理员有用的三个过滤器？

2. Wireshark 在生产网络中的其他使用方式是什么？
