视频 - Wireshark 中的 IPv4 报头示例（6 分钟）

让我们看看如何查看和分析一个 Wireshark 数据包捕获中的网络层信息。在 Wireshark 中捕获的数据包的网络层信息。我有一张来自一个 Wireshark 数据包捕获的屏幕截图。可以看到捕获的第二个数据包已高亮显示。然后在数据包详细信息窗口中，已展开网络层信息以向我们展示网络层发生的所有事情。

下面看看我们检查的这个数据包中发生了什么。我们可以看出，首先，我们使用的网络层协议或 Internet 层协议是 Internet 协议第 4 版 (IPv4)。我们也可以看到源 IP 地址是 192.168.1.109。也可以看到它已在数据包列表窗口区域中的这里高亮显示，并且目的 IP 地址是 192.168.1.1。我们也可以在这里看到。我们可以看到，在更高的层上，这是 TCP 协议数据包。但是如果我们仅限制到 IPv4 字段或 IPv4 信息，我们可以看到每个 IPv4 数据包中包含的不同类型的控制信息。

例如，版本号（是 4）表明这是 IPv4，而不是 IPv6 数据包。报头长度--这是 IPv4 报头的最小大小。差异化的服务字段（用于确定数据包的优先级）对 IP 电话等应用很有用。数据包的总长度、标识编号用于分段。标志，可以看到 DF 位已设置，这表示“不分段”。此数据包不够大或未识别出需要分段。分段偏移量，TTL 或生存时间，设置为 128。每次将一个数据包从一个跃点路由到下一个跃点时，每次将一个数据包从一跳路由到下一跳时，TTL 编号会减少。TTL 数会减少。当 TTL 编号到达 0 时，当 TTL 数字为 0 时，该数据包就会被丢弃，确保该数据包不会无止境地在 Internet 上传播。TTL 值也可用在 ICMP 跟踪路由和 ping 中。协议字段告诉我们数据包的数据部分需要的信息类型。6 表示这个数据包的数据部分是一个 TCP 数据包。报头校验和字段，允许路由器检查 IP 报头中是否有任何错误或不一致性。如果有，将丢弃该数据包。

最后是源和目的 IP 地址，它们是 IPv4 数据包的最重要部分。我们看看 Wireshark 数据包捕获的另外两个屏幕截图，我们将看到一些异同点。下一个屏幕截图表明现在我们看到的是捕获的第 8 个数据包。该数据包的源 IP 地址也是 192.188.1.109，目的 IP 地址是 192.168.1.1，但此数据包是 HTTP GET 请求。所以这是对位于 192.168.1.1 的 Web 服务器的请求。可以看到网络层或 Internet 层信息已展开，这也是 IPv4 协议，而且我们在不同的字段中有类似的信息。

可以在总长度字段下注意到此数据包有 411 字节，而前一个数据包仅有 52 字节。您可以看出此数据包包含更多的信息，或者是一个比前一个包大得多的包。如果查看下方的 Internet 协议第 4 版信息，我们可以看到 TCP 信息，在其下方是超文本传输协议或 HTTP 协议，也是此数据包中的信息。继续看下一个数据包，可以看到此数据包是捕获的第 16 个数据包，它就在这里。它也是从主机 192.168.1.109 发送到主机 192.168.1.1 的，但这是 ICMP 协议。从数据包列表窗口中的信息可以看到这是一条回应或 ping 请求。如果我们查看详细信息区域中的 Internet 协议第 4 版信息，可以看到一些细微差异。仍为第 4 版。报头长度仍为 20 字节。但我们可以看到标志稍有不同，协议字段现在设置为 1，表明此数据包的数据部分是一条 ICMP 协议消息。可以在详细信息窗口的底部注意到，这个展开区域显示了特定于 ICMP 的报头信息。