在語音和影片呼叫的Wireshark中解密RTP流以進行丟包分析

目錄

[簡介](#)
[問題](#)

簡介

本文說明如何破解即時流(RTP)流，以便在語音和影片呼叫的Wireshark中進行資料包丟失分析。您可以使用Wireshark過濾器來分析在呼叫的源和目標處或靠近源處捕獲的同步資料包。當懷疑網路丟失時，您必須排除音訊和影片品質問題，這一點很有用。

問題

此示例使用此呼叫流：

IP電話A（中央站點A）> 2960 switch > Router > WAN router（中央站點）> IPWAN > WAN router（站點B）> Router > 2960 > IP電話B

在此方案中，遇到的問題是從IP電話A到IP電話B的影片呼叫會導致從中心站點A到分支站點B的影片品質變差，其中中心站點品質較好，但分支站點出現問題。

檢視分支IP電話的流統計資料中的接收方丟失的資料包：

解決方案

品質僅在分支站點上可見，並且由於中心站點看到的是一個好的影象，因此從中心站點到分支站點的流似乎正在通過網路丟失資料包。

```
IP addressing scheme
Central IP phone: 192.168.10.146
Central Gateway: 192.168.10.253
```

```
Central WAN router: 192.168.10.254
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231
```

資料包捕獲在中央和分支WAN路由器上進行，WAN丟棄這些資料包。關注從中央IP電話(192.168.10.146)到分支IP電話(192.168.207.231)的RTP流。 如果WAN丟棄從中央WAN路由器到分支WAN路由器的資料流上的資料包，此資料流會丟失分支WAN路由器上的資料包。請使用wireshark中的過濾器選項來隔離問題：

1. 在wireshark中開啟捕獲。

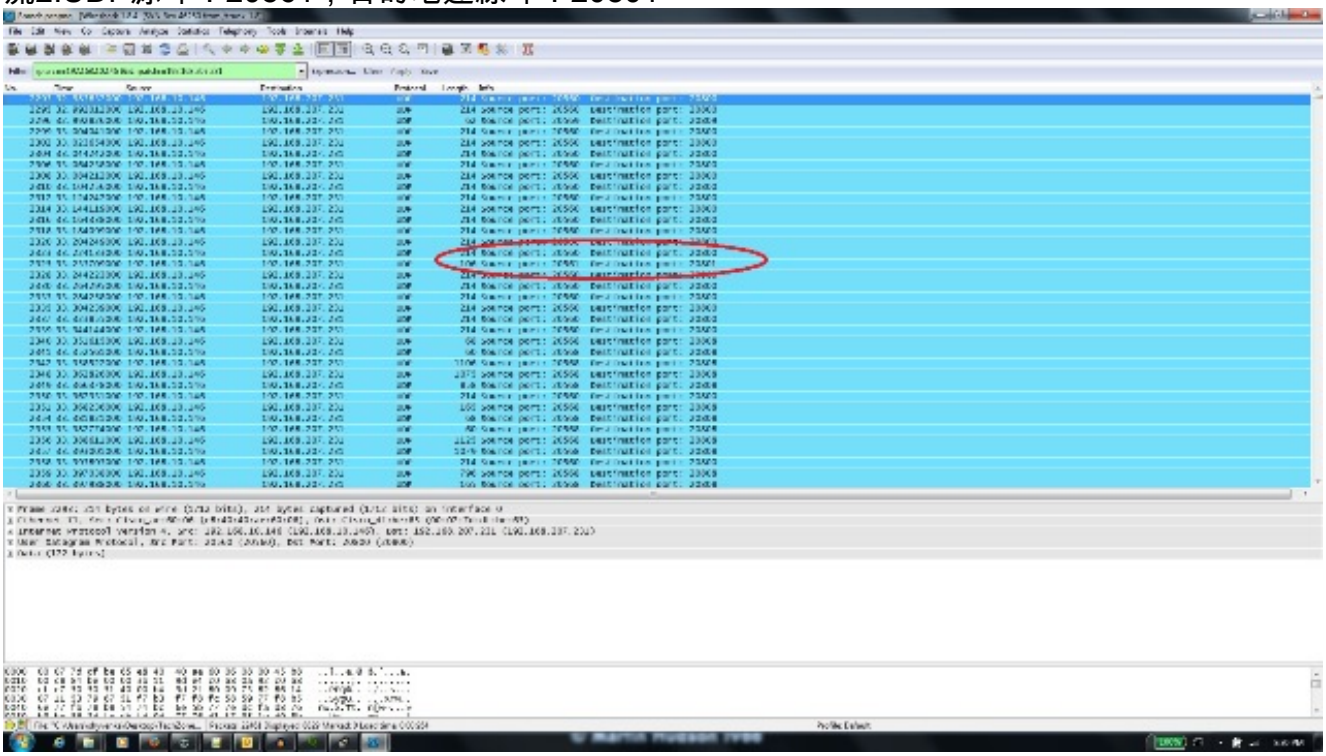
2. 使用過濾器ip.src==192.168.10.146 && ip.dst==192.168.207.231。這將過濾掉從中央IP電話到分支IP電話的所有UDP資料流。

3. 僅對分支側捕獲執行分析，但請注意，還必須對集中捕獲執行這些步驟。

4. 在此螢幕截圖中，UDP流在源IP地址和目標IP地址之間過濾，並包含兩個UDP流（由UDP埠號區分）。 這是一個影片呼叫，因此有兩個流：音訊和影片。在本示例中，兩個流是：

   流1 :UDP源埠：20560，目的地連線埠：20800

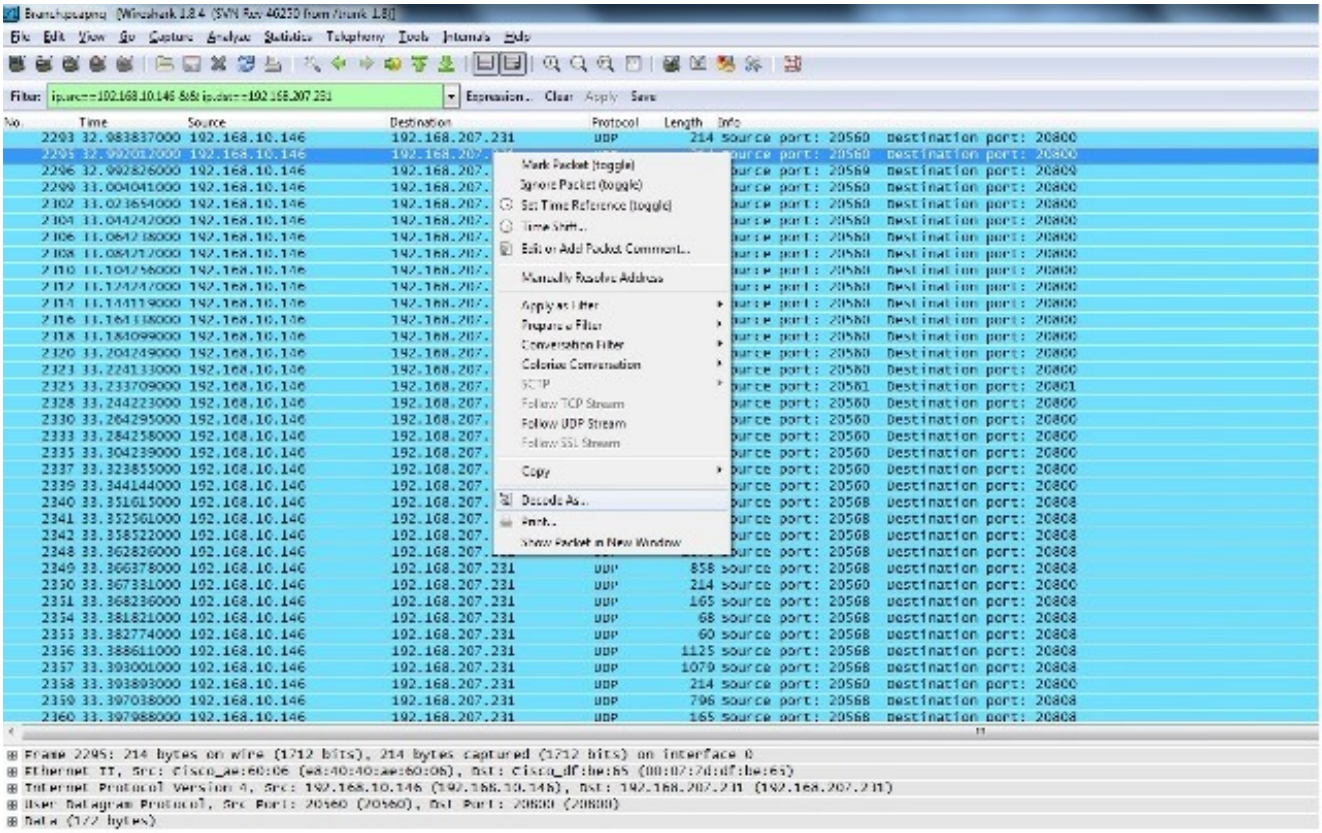
   流2:UDP源埠：20561，目的地連線埠：20801



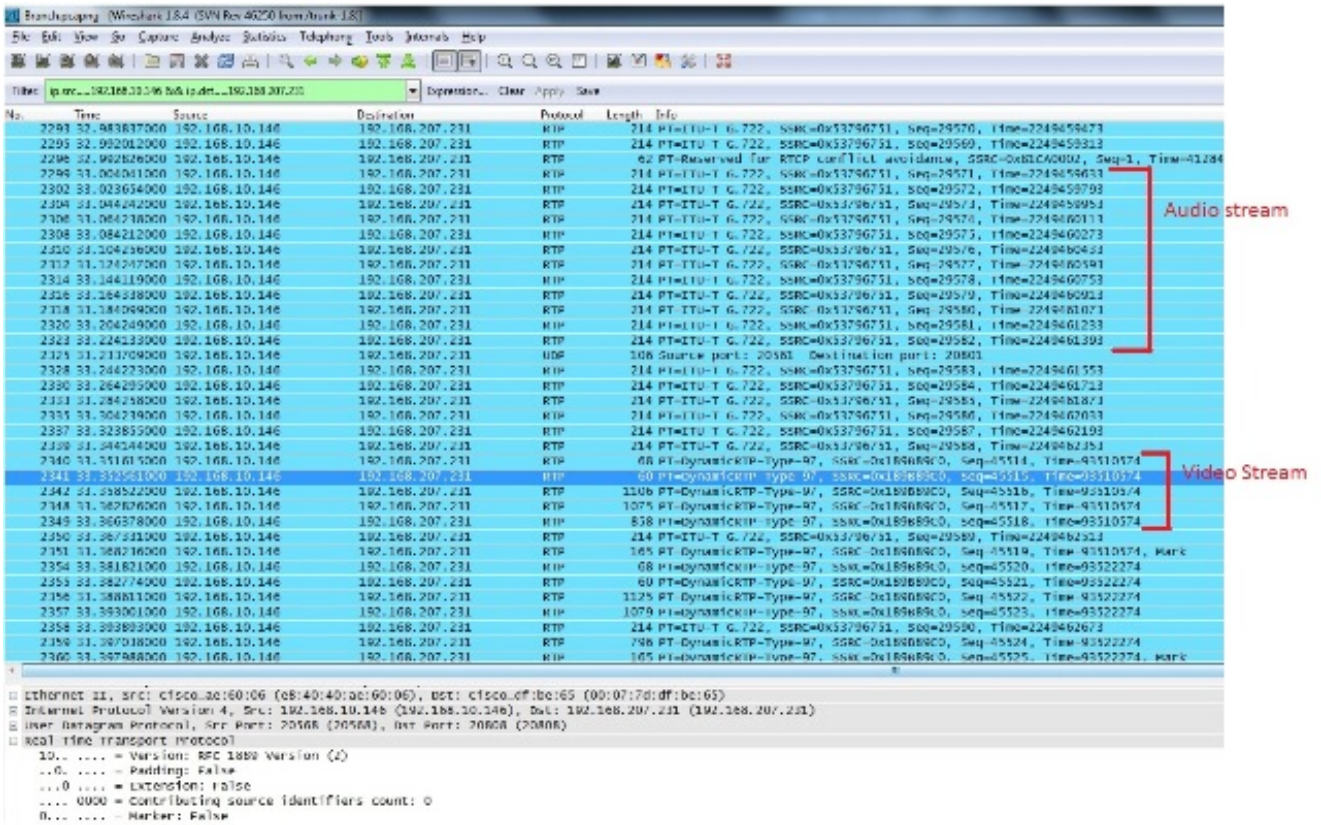
5. 從其中一個流中選擇資料包，然後按一下右鍵該資料包。

6. 選擇**Decode As...**並鍵入**RTP**。

7. 按一下「**Accept**」和「**Ok**」，將串流解碼為RTP。

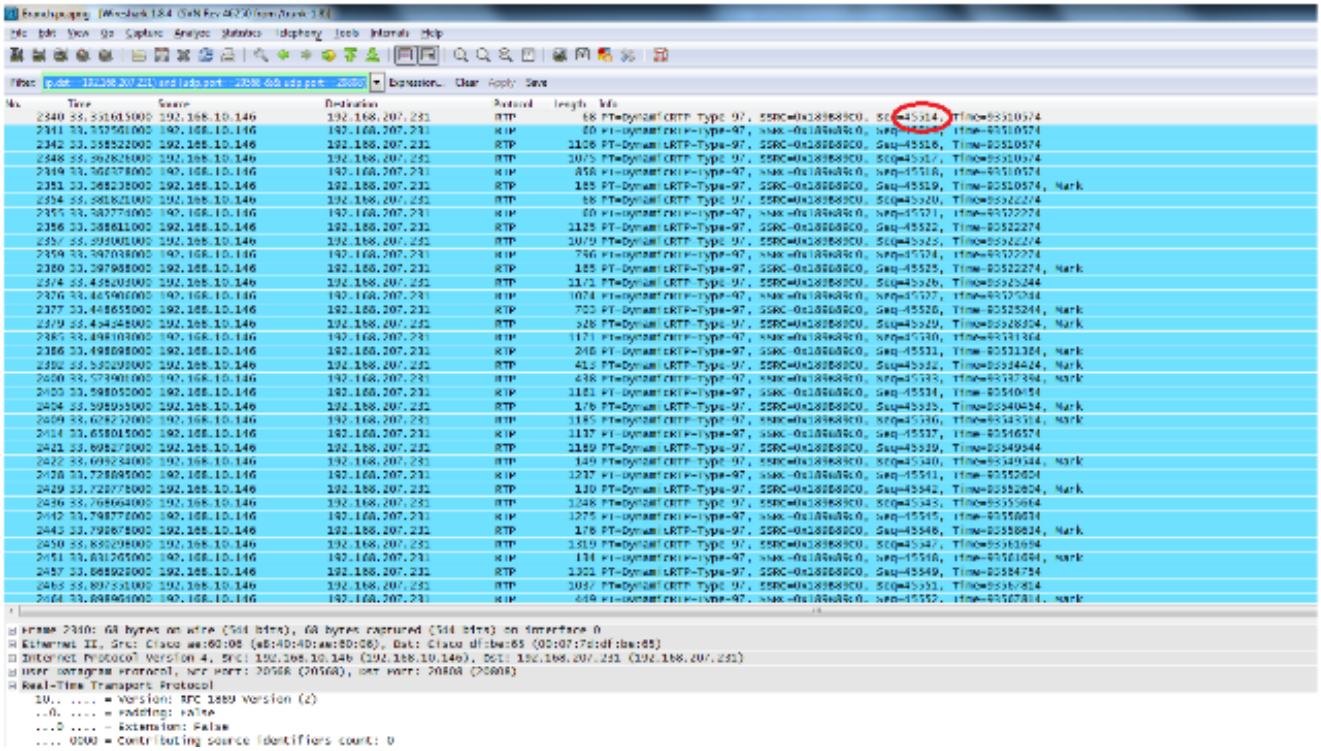


剩下的一個流被解碼為RTP，另一個流被解碼為未編碼的UDP。



8. 從未編碼流中選擇一個資料包，並將其解碼為RTP。這會將音訊和影片流解碼為RTP。

註：音訊流採用G.722編解碼器格式，Dynamic-RTP-97負載型別表示影片RTP流。

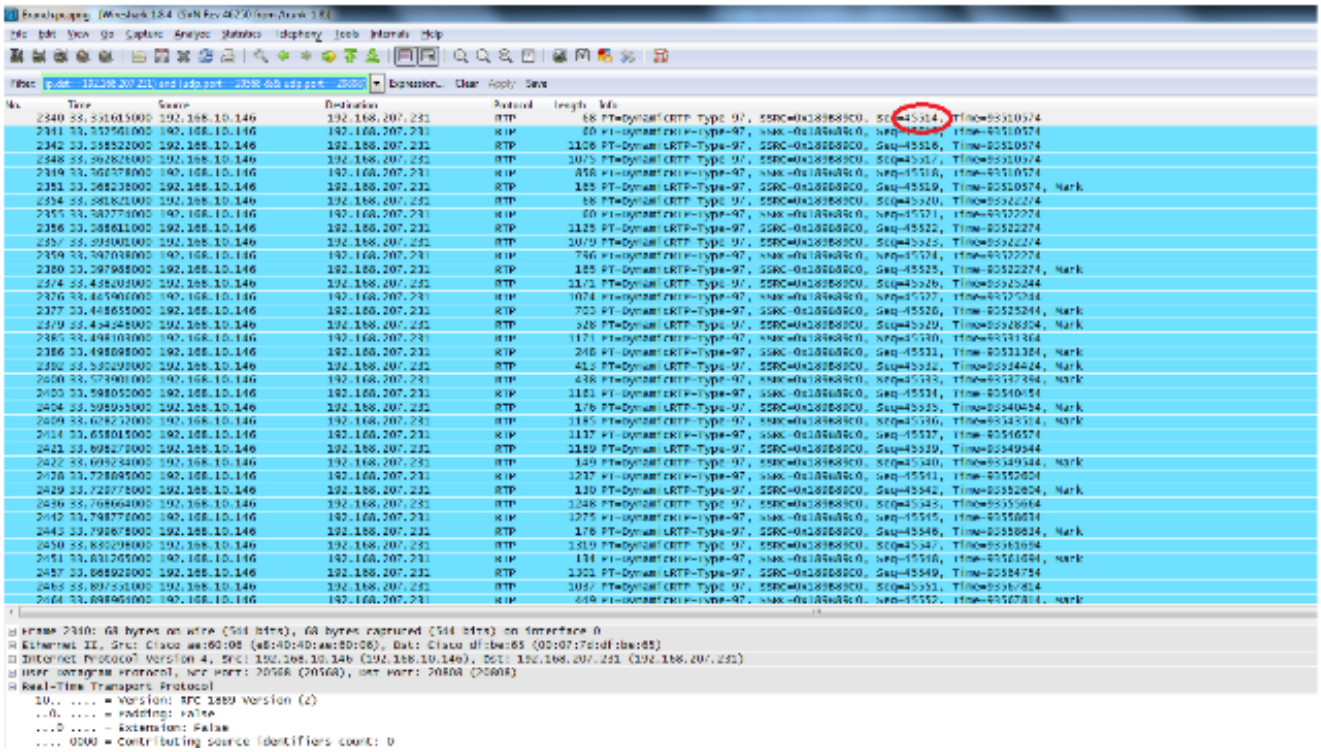


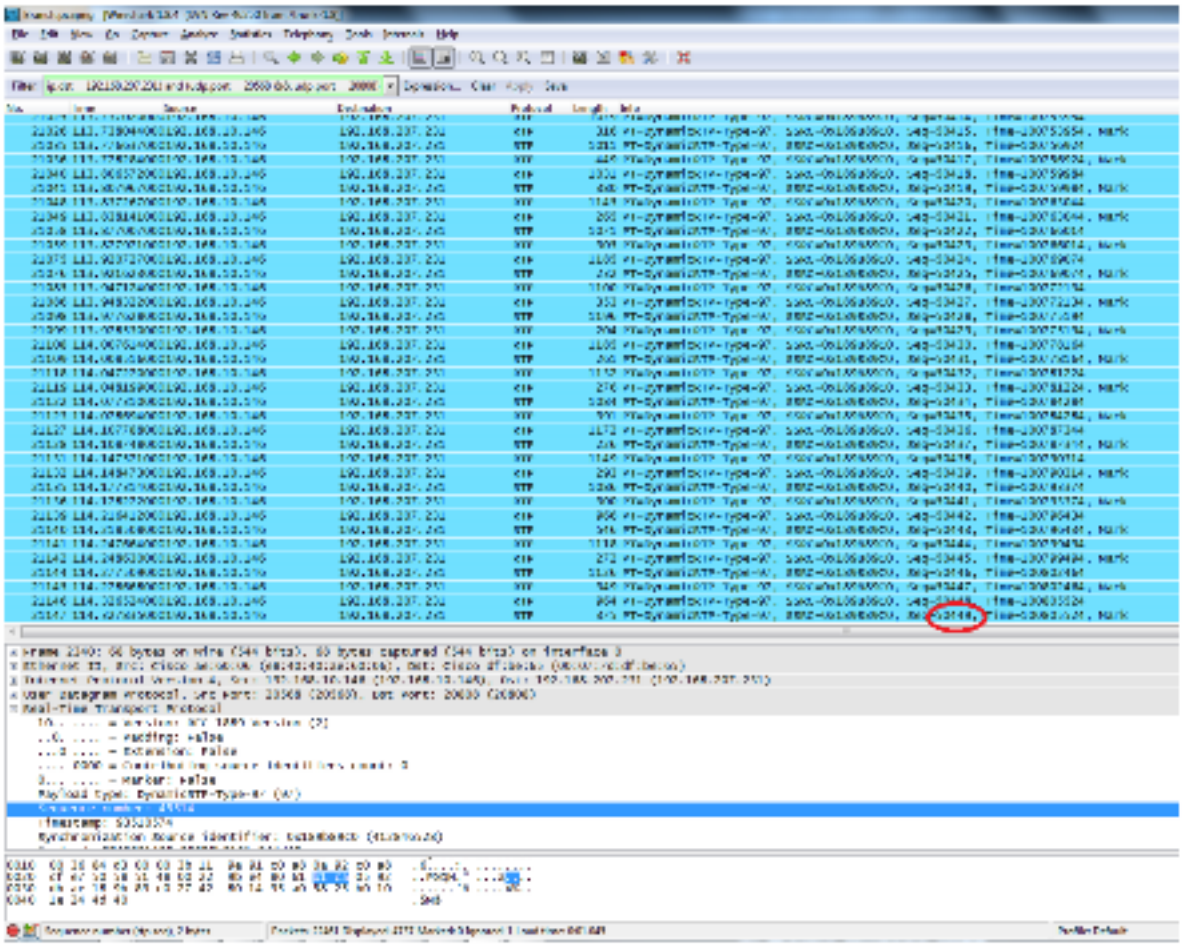
現在問題只在於影片品質。關注影片RTP流，並使用此流的UDP埠號過濾掉其他流。

9. 在Wireshark實用程式的底部窗格中選擇一個顯示UDP埠資訊的資料包，以檢視埠號。在上一個螢幕截圖中，選擇了來自影片流的一個資料包，您可以在底部窗格中看到Src Port(20568)和Dst port(20808)資訊。

   提示：使用以下過濾器：(ip.src==192.168.10.146和& ip.dst==192.168.207.231)&(udp.port eq 20568和udp.port eq 20808)。 您只能看到此螢幕截圖中所示的影片RTP流。

   附註：記下此流的第一個和最後一個RTP序列號。





第一個RTP序列號是45514而最後一個RTP50449號是過濾出的影片RTP流。

10. 確保兩個捕獲中都有第一個和最後一個RTP序列號資料包（例如，中央捕獲和分支捕獲），並注意兩個捕獲上流的SSRC相同。
11. 最佳化過濾器以僅匹配第一個和最後一個RTP流之間的資料包。

    序列號用於最佳化資料流，以防捕獲不是同時捕獲，而是稍微延遲。

    附註：分支站點可能在IP後啟動一些序45514。

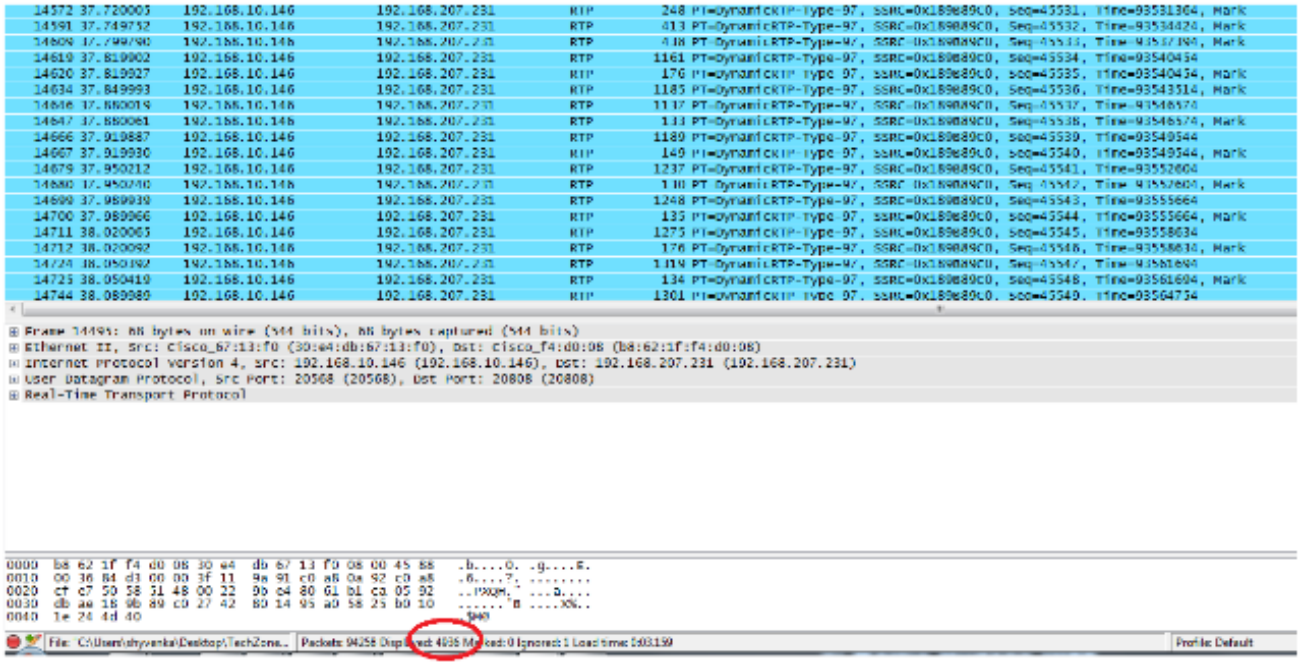
12. 選擇開始和結束序列號。這些封包同時存在於擷取和縮小篩選條件中，以僅顯示開始RTP序列號和結束RTP序列號之間的那些封包。此方法的篩選器為：

```
(ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568
and udp.port eq 20808) && ( rtp.seq>=44514 && rtp.seq<=50449 )
```

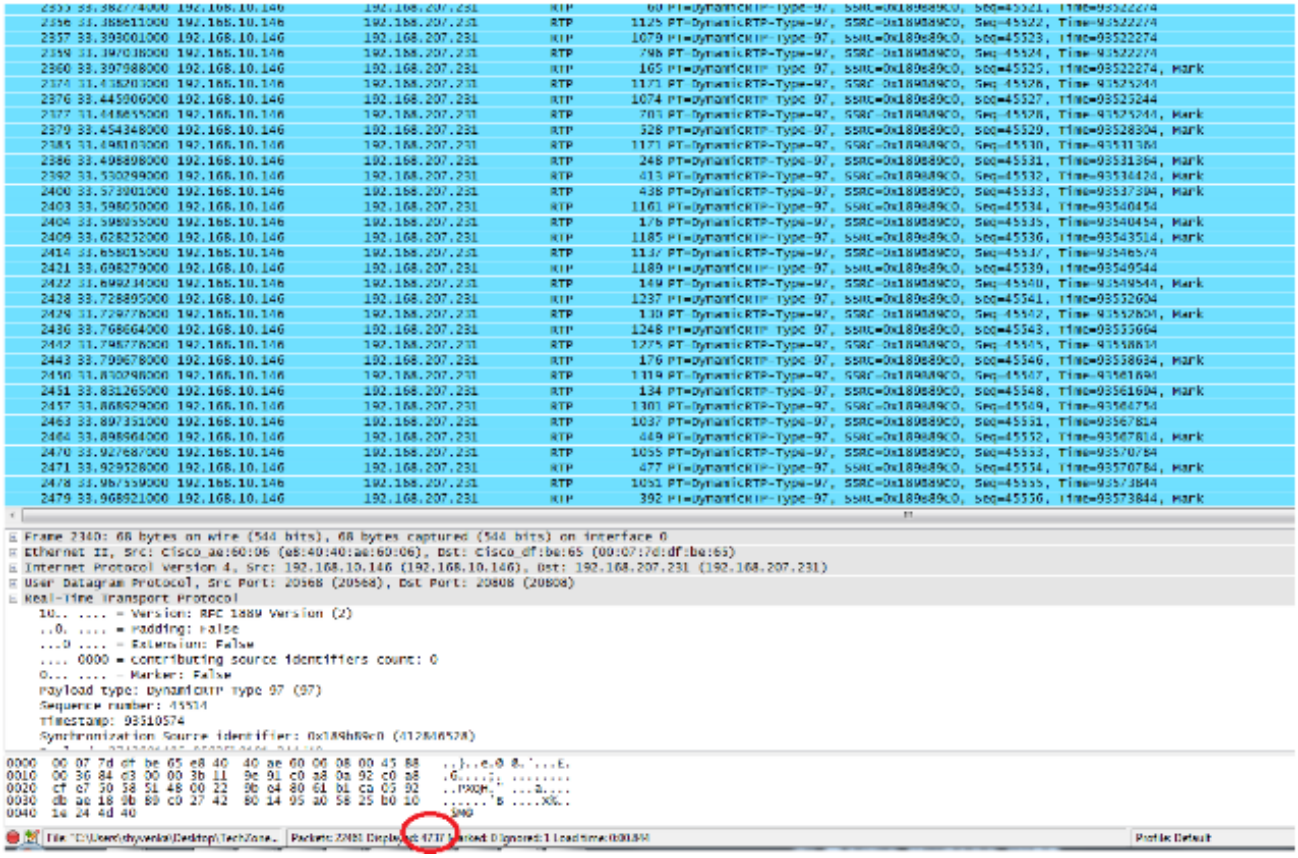
    同時進行擷取時，兩個擷取的時刻開始或結束時不會遺漏封包。如果您看到其中一個擷取在開始/結束時不包含幾個封包，請使用兩個封包中遺失的擷取中的第一個序號或最後一個序號，來精簡兩個擷取的篩選條件。觀察在相同序列號（RTP序列號範圍）之間的兩個點捕獲的資料包。

    應用過濾器時，您會在中心站點和分支站點看到以下內容：

中心站點：



分支站點：



請注意Wireshark實用程式底部窗格中兩個捕獲上的過濾資料包計數。**Displayed**計數表示與所需過濾條件匹配的資料包數。

中心站點有4,936個資料包符合開始(45514)和結束(50449)RTP序列號之間的期望過濾標準，而分支站點只有4,737個資料包。這表示丟失199個資料包。請注意，這199個資料包與本文檔開頭所示的分支端IP電話的流統計資訊中的「Rcvr Lost Pkts」計數匹配199。

這確認所有Rcvr丟失的資料包實際上是通過WAN丟棄的網路丟失。這就是在處理涉及可疑網路丟棄的音訊/影片品質問題時隔離網路中丟包點的方式。