

## 协作设备抓包后提取 H263, H264 视频流

在协作设备的排错过程中，大多数时候我们得到了呼叫的抓包文件，只专注于分析丢包率、流控信息等其它对于排错关键的数值信息。

为了得到更加直观的信息来进行排错。通过我的多次尝试，只要我们写出对应的 SDP 文件并且导入 VLC 播放器，再使用 rtptools 作为媒体服务器播放，就能模拟数据包内的 RTP 流，向本地播放器发送视频信号。

不论是双流信号还是双向的视频流信号，都能被轻松解码成本地播放器能够播放的视频。

### 使用情形

解码数据包内 RTP Stream 承载的视频流，并且在本地播放以验证清晰度、传输质量等。

目前主流的视频编解码协议是 H263 和 H264，但 H264 更常用。

本方法适用于 SIP 发起的未加密的呼叫：SIP over TCP/UDP

### 原理

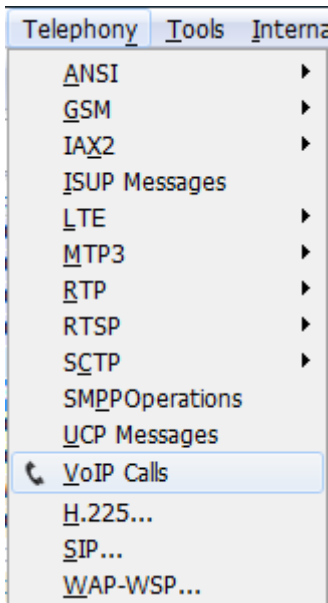
1. 提取数据包中的 RTP 流，保存为 rtpdump 文件，使用 rtptools 包含的 rtpdump 工具打包成 rtplay 工具能够播放的文件，并且使用 rtplay 工具作为服务器在本地播放这个 RTP 流。
2. 根据数据包内的 SDP 信息编写对应的 SDP 文件，使用 VLC 播放器打开这个 SDP 文件作为客户端接收 rtplay 发来的 RTP 流，解码并播放视频。

### 所需工具

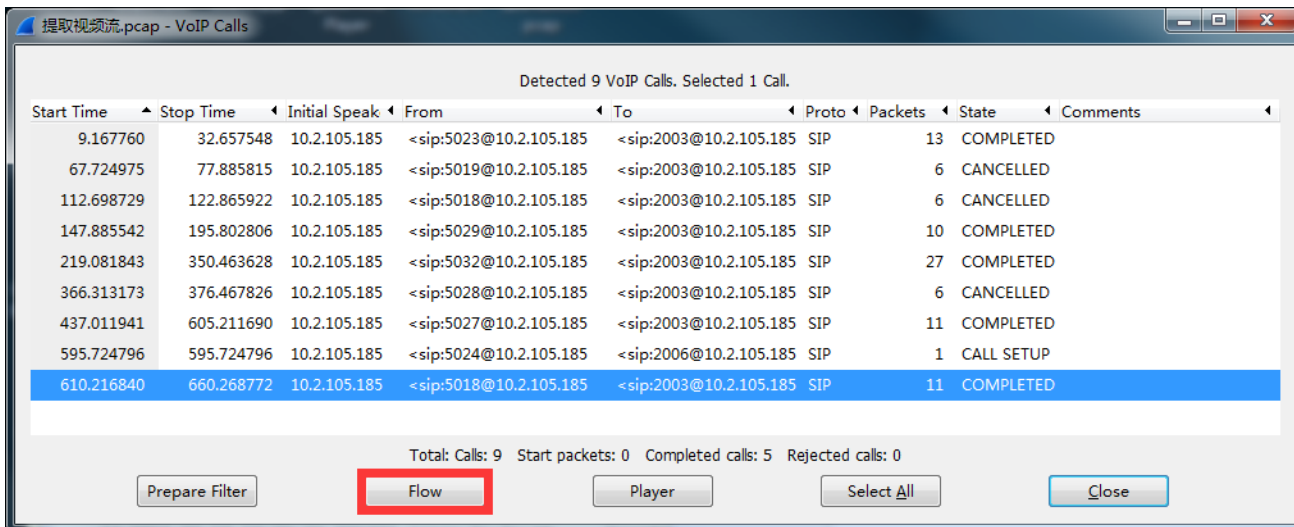
1. Wireshark
2. rtptools  
下载地址：<http://www.cs.columbia.edu/irt/software/rtptools/download/>
3. VLC 播放器  
下载地址：<http://www.videolan.org/>

## 操作过程

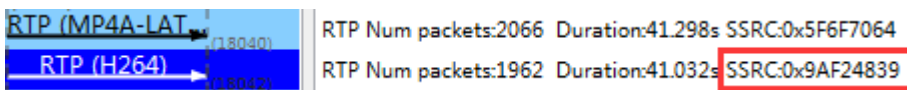
1. 从 Wireshark 提取 RTP Stream, 打开待分析的包, 点击:



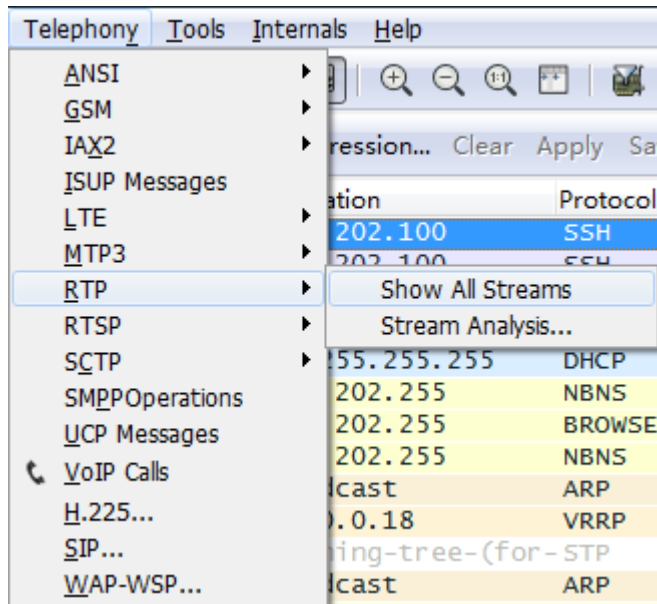
选中需要分析的呼叫, 点击 Flow:



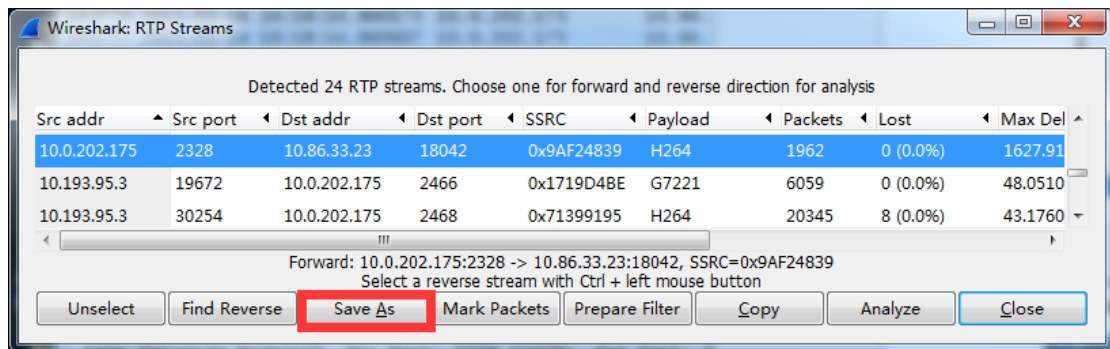
记录 H264 对应的 SSRC:



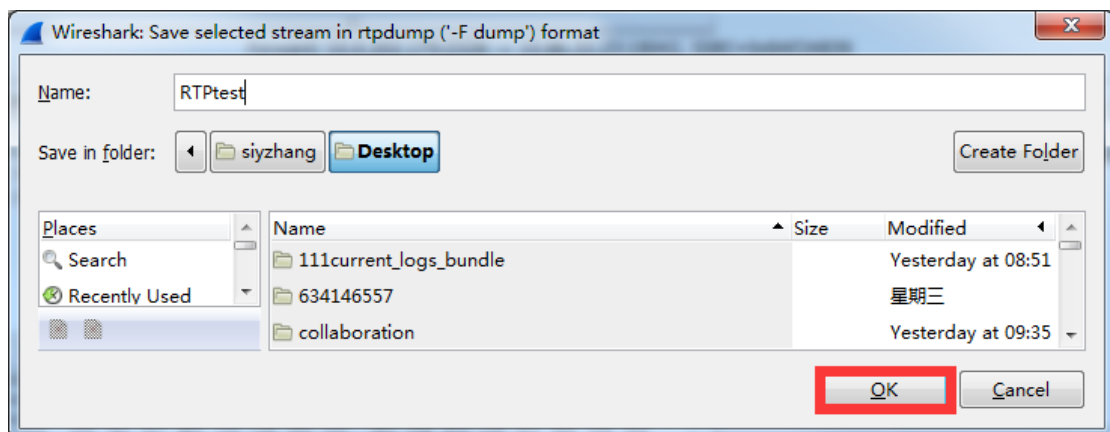
打开 RTP>>Show All Streams



通过 SSRC 找到对应的 H264 流，点击 Save As



取个名字，不带后缀名，点击 OK。



- 打包 RTP 流；打开 Windows 的命令行，切换到 rtpools 的目录，或者预先将此目录加入 Path 变量中

```
C:\Users\siy Zhang>cd Desktop\rtpools_1_18_win_bin
C:\Users\siy Zhang\Desktop\rtpools_1_18_win_bin>
```

使用 rtpdump 工具打包 RTP 流，成为 rtplay 工具可播放的格式：

```
rtpdump -F dump -f ..\RTptest -o RTptest.rtp
```

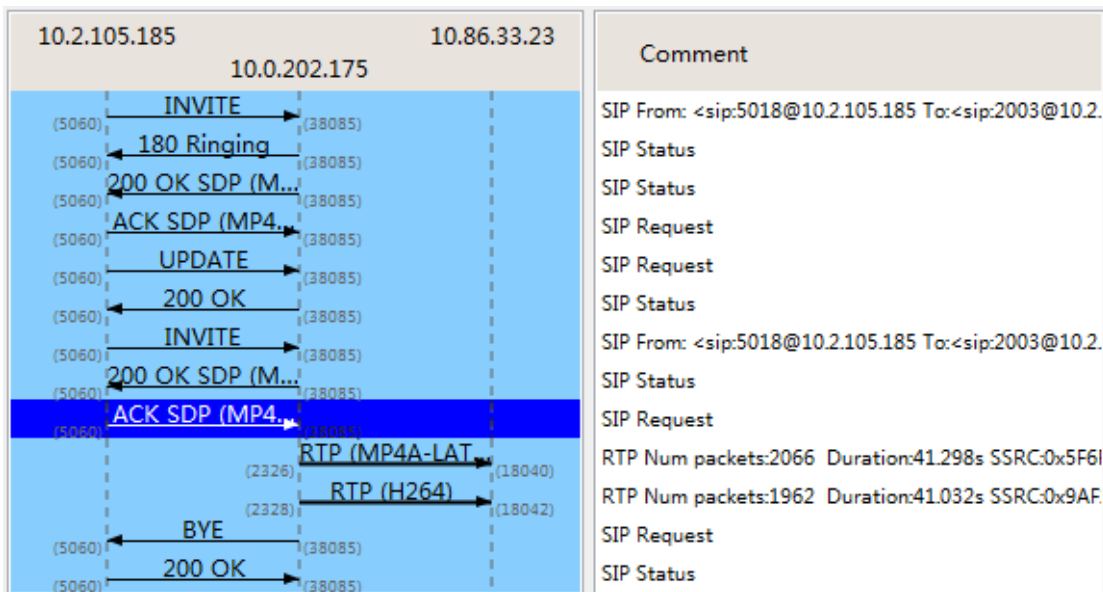
-F 参数指定 payload 类型

-f 参数指定源文件

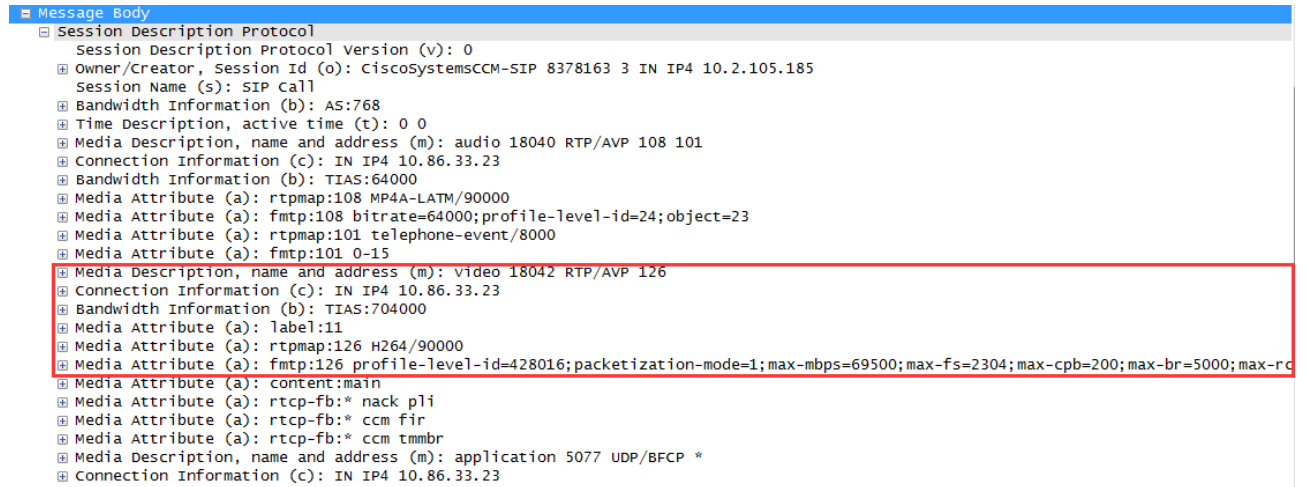
-o 参数指定目标文件

```
C:\Users\siy Zhang\Desktop\rtpools_1_18_win_bin>rtpdump -F dump -f ..\RTptest -o
RTptest.rtp
C:\Users\siy Zhang\Desktop\rtpools_1_18_win_bin>
```

- 编写 SDP 文件，使用 Wireshark 查看这通呼叫的最后一个 ACK SDP 消息：



根据 SDP 中的 Video 信息，编写一个最简单的 SDP 文件，用于 VLC 播放器作为客户端接收媒体流。



testRTP.sdp //在 127.0.0.1:5002 接收 H264 视频流

```
m=video 5002 RTP/AVP 126
c=IN IP4 127.0.0.1
a=rtpmap:126 H264/90000
a=fmtp:126          profile-level-id=428016;packetization-mode=1;max-mbps=69500;max-
fs=2304;max-cpb=200;max-br=5000;max-rcmd-nalu-size=884736;max-smbps=69500;max-
fps=6000
```

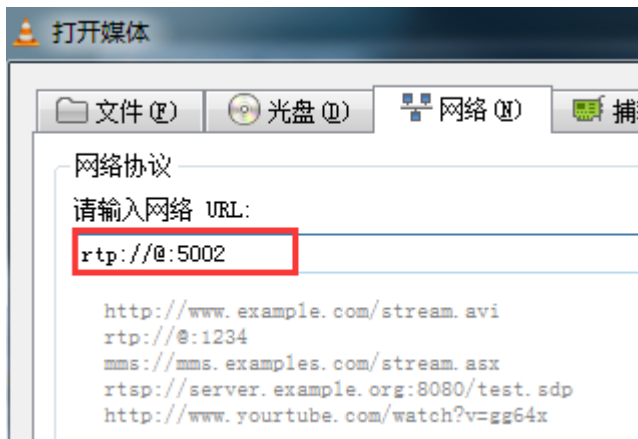
```
m=video 5002 RTP/AVP 126
c=IN IP4 127.0.0.1
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=428016;packetization-mode=1;max-mbps=69500;max-fs=2304;max-cpb=200;max-br=5000;max-rcmd-nalu-size=884736;max-smbps=69500;max-fps=6000
```

- 使用 VLC 导入 SDP 文件，并开始播放（因为 RTP/RTCP 需要校验包头，需要先打开客户端）

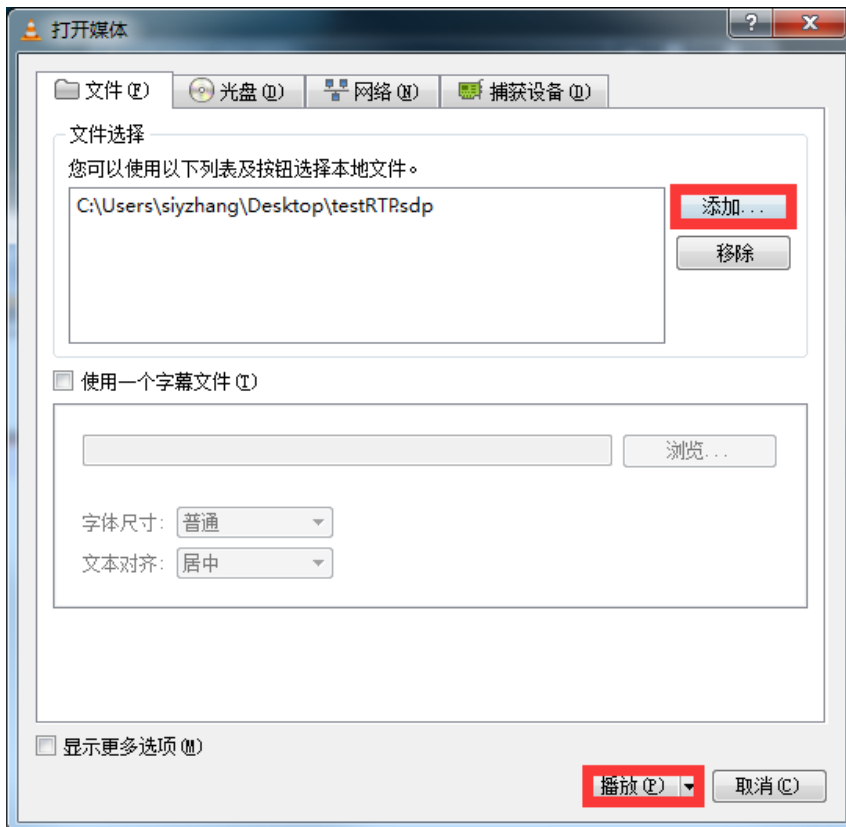
点击打开网络串流:



按下图进行设置并且添加刚刚编写的 SDP 文件。



设置完成后点击播放:

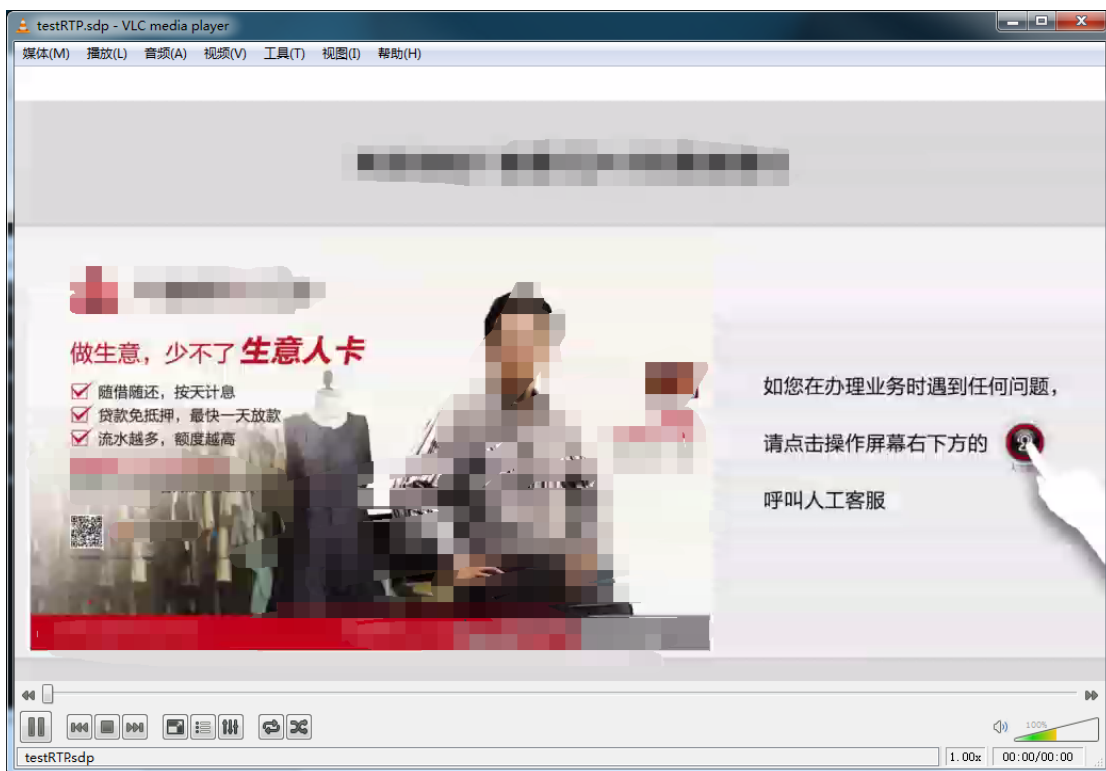


5. 使用 rtpplay 作为服务器端发送视频流，在 127.0.0.1:5002 发送

```
C:\Users\siy Zhang\Desktop\rtp tools_1_18_win_bin>rtpplay -T -f RTPtest.rtp 127.0.0.1/5002_
```

```
rtpplay -T -f RTPtest.rtp 127.0.0.1/5002
```

回车后可以看到 VLC 播放器开始正常播放视频:



## 扩展

如果需要加入音频流，可以在 SDP 文件中加入对应的行，并且再开启一个命令行窗口运行 rtpplay 工具来发送音频即可。

是不是非常有趣~~我正在研究使用这种方式播放更多的视频，还有如何使用 Wireshark 解码出 H264 的裸码流，可以直接使用比如“暴风影音”这样的软件直接播放。

关于更多 RTP 的知识，请参考 RFC1889

<https://www.ietf.org/rfc/rfc1889.txt>