Wireshark RTP Audio Capture Process

Why is an Audio Packet Capture Required?

An RTP audio packet capture gives us the information needed to design the best solution possible based on your current or future planned infrastructure. The capture tells us what call data element events (Metadata) are being passed from the IP PBX to the IP Phones. The capture also provides data elements from a CTI Server (if available). With this information we're able to:

- Determine the best tap point on your network for call recording
- Provide you with what information you'll be able to capture and attach to call records for search, retrieval & playback
- Access if there are any data element gaps
- Determine if any network architecture changes are needed to resolve any data element gaps
- Determine if a specific Application Protocol Interface (API) is required

What do I need to do prior to getting the RTP Audio Capture?

1) Determine if you are using Port Mirroring on your network

Port Mirroring, also known as SPAN (Switched Port Analyzer) is a method of monitoring network traffic. With port mirroring, the network switch sends a copy of all packets seen on one port, to another port, where the packets can be analyzed. Port Mirroring allows other computers to see network traffic which is not otherwise visible to them. Port Mirroring is a standard feature in nearly all enterprise class managed switches/layer 2 Ethernet switches. There is a configuration interface which is used to specific the source port to be mirrored and the destination port, where copy of all ports will be forwarded.

An example of a SPAN configuration on a Cisco 2950 Switch:

```
Monitor session 1 source interface fast ethernet 0/1, 0/2, 0/3
Monitor session 1 destination interface fast ethernet 0/4 encap ingress Vlan 1
```

In this example data is mirrored from ports 0/1, 0/2 and 0/3 to destination port 0/4 using Vlan1 for Vlan tagging. To show status of a SPAN monitor session use the following command.

```
Show monitor session 1
```

In order for us to provide a port mirroring (SPAN port) call recording solution it is important to validate that your network switches support port mirroring capabilities. If you are unclear, please check the manufacturer's documentation and confirm Port Mirroring/SPAN is provided. This functionality is also used when gathering a RTP Audio Capture.

2) Determine your RTP Capture Points

Selecting RTP audio capture points are an important part of this process and should be discussed with your Project Manager upon review of a Local or Wide Area Network diagram.

Four types of captures are required for assessment and review:

1) Internal Station to Station call
2) Outbound call
3) Inbound call
4) Conference cal

Note: Each capture should be a minimum of 1 minute and be given a file name that relates to the capture call type like *YourCompanyName_OutboundCall.pcap*. Additionally, it is very beneficial that when recording a test capture that you verbally indicate the type of test capture like "*Hi, this is Bob, I am doing a test call for gathering an audio capture sample. This call is a station to station call from ext 2456 to 3789.*"

Download and install the Wireshark application

The Wireshark application is a free application and can be downloaded at the following URL address:

https://www.wireshark.org

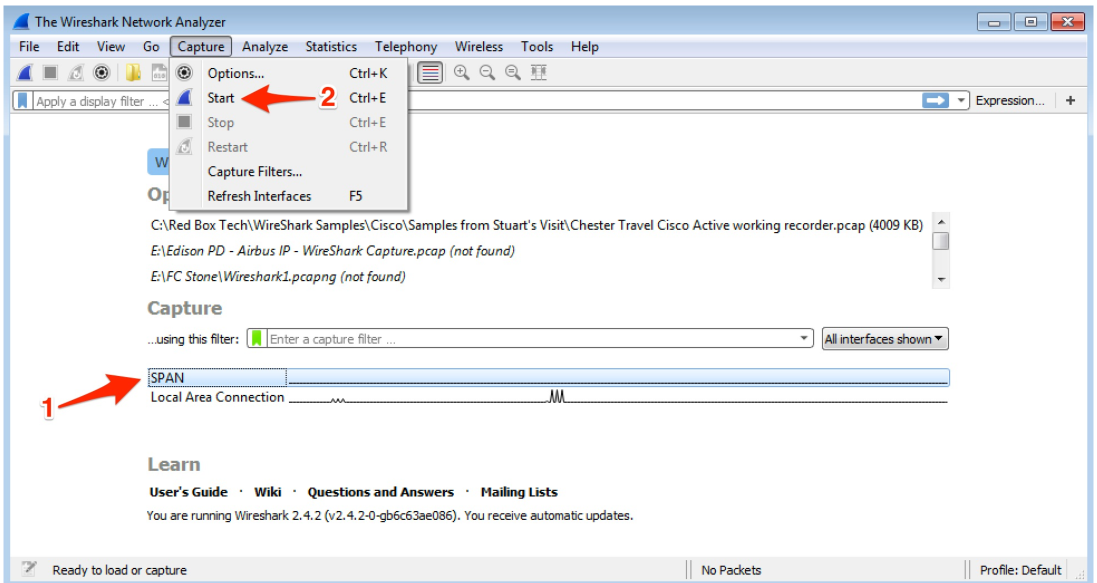
When installing Wireshark, select all the default settings and launch the application when installation is complete.

Wireshark RTP Audio Capture Process

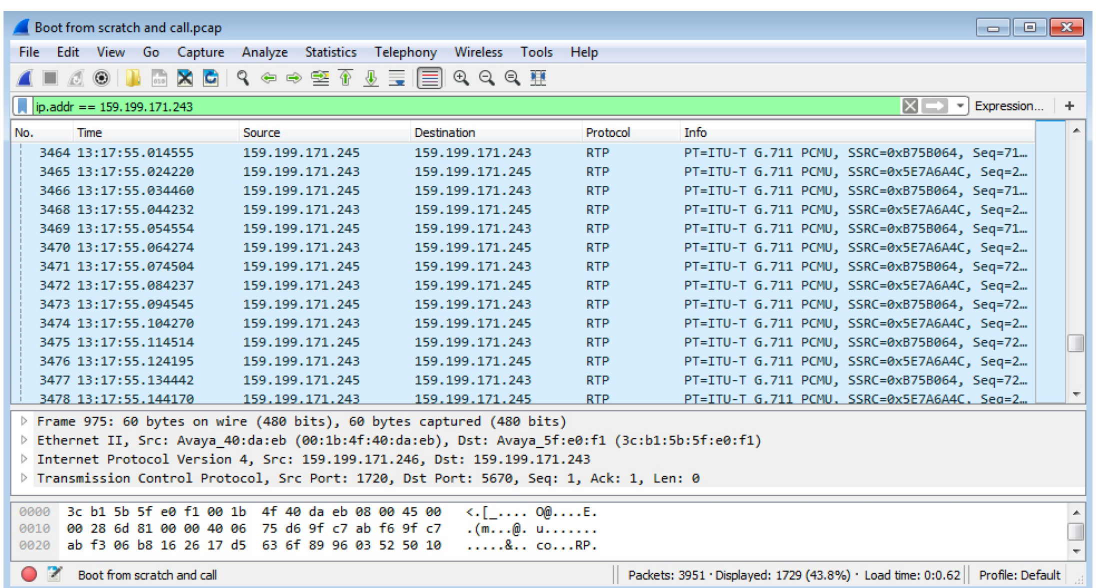
How do I obtain the RTP Audio Capture?

Step One) Open the Wireshark application.

(1) Select/Highlight the Network Interface Card (NIC) used for the SPAN session.
(2) From the **Capture** menu at the top select, **Start**.



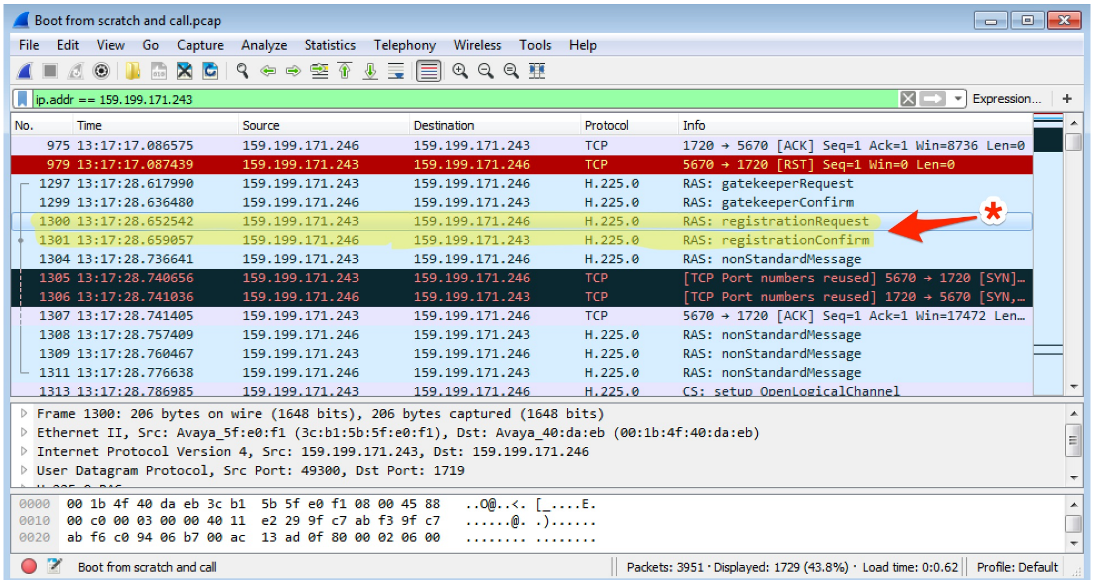
You will now start to see numerous events and protocols streaming through. RTP is the protocol we're most interested in.



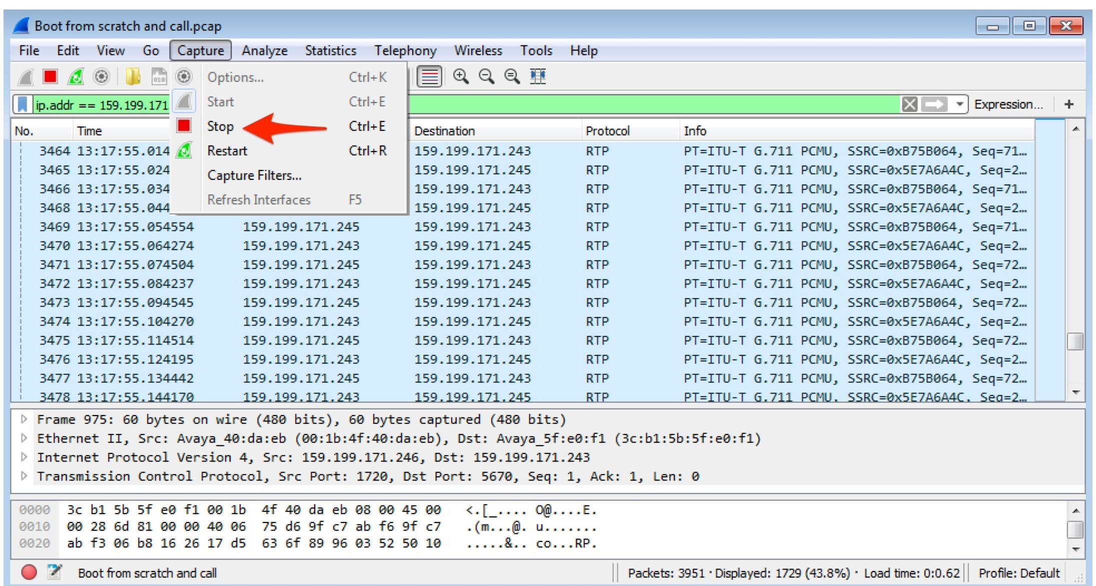
Wireshark RTP Audio Capture Process

Step Two) While the trace is running perform the following.

<u>Reboot</u> the phone device that will be tested *(to capture its registration* with the IP PBX)*, making a note of its extension, IP Address and time of reboot. When the device has restarted, log in to it and make an outbound call to another number such as a mobile. Talk briefly (30 sec to 1 min) and then hang up the call.

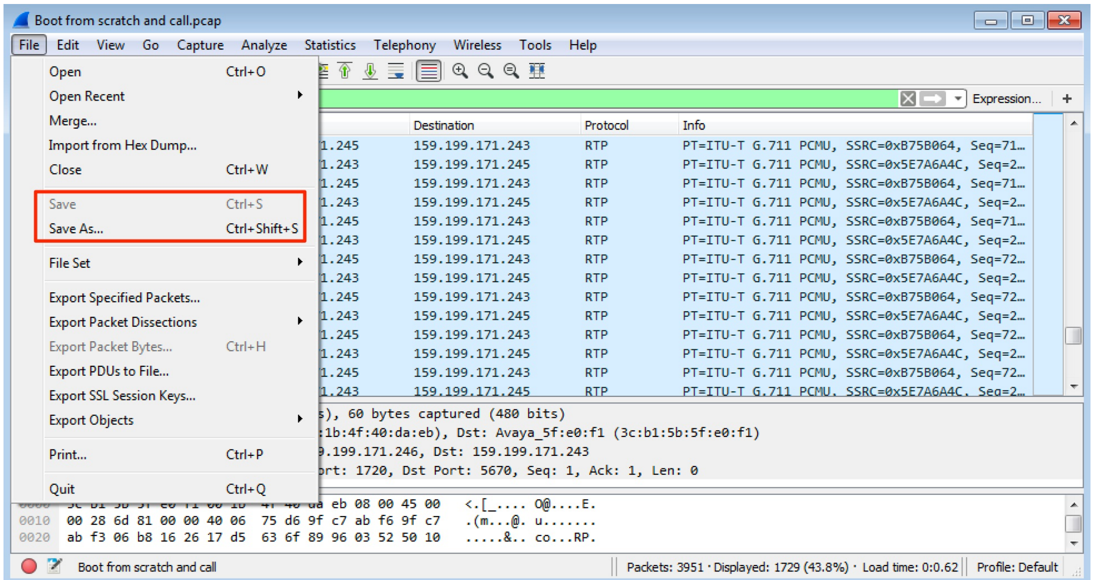


Step Three) Now go to the **Capture** menu and select **Stop**



Wireshark RTP Audio Capture Process

Step Four) From the **File** menu, save the file giving it a name such as 'Boot from scratch and call.pcap'



Step Five) Next *(utilizing previous Steps but skipping Step Two)*, obtain Wireshark captures for the following 4 test scenarios.
Note:

- *A separate Wireshark capture file should be created for each test.*
- *Make sure to complete each test scenario before stopping the capture file.*
- *After conducting each test, assign a name to each Wireshark capture file using the examples below.*

Test #1: Place a 1 minute call from Device #1 to Device #2. Device #2 accepts call.
Wireshark filename example: "CompanyName_Test1_Internal.pcap"

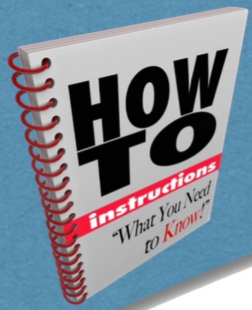
Test #2: Place a 1 minute call from Device #1 to an external number. External participant accepts call.
Wireshark filename example: "CompanyName_Test2_Outbound.pcap"

Test #3: Place a 1 minute call from external number to Device #1. Device #1 accepts call.
Wireshark filename example: "CompanyName_Test3_Inbound.pcap"

Test #4: Place a 1 minute call from Device #1 to Device #2. Then conference in an external number/participant.
Wireshark filename example: "CompanyName_Test4_Conf.pcap"

Once the 4 captures are complete, please send all 5 pcap files to us to start the assessment process.

Thank you for all your effort in providing this valuable information for our engineers to evaluate and come up with the best solution for your environment.



Troubleshooting Tips

Avaya SPAN

If you are using Avaya SPAN and are having difficulties capturing an audio stream, please check the following items:

1) Is Signaling Encryption turned off?
   In the ASA IP-Network-Region, Page 2, ensure the H.323 SECURITY PROFILES is configured to “Challenge”.

2) Is Direct IP-IP Audio connection off?
   In ASA STATION, page 2, ensure the Direct IP-IP Audio Connections? Is set to “N”.
   (Note this setting forces RTP to go through media gateway if station to station call)

For additional inquiries you can contact us at:
support@interactionic.com
(800) 285-2950