It is assumed that the PacketScan™ Analyzer Software and License installations are already performed referring to the Software Quick Installation Guide (Packetscan-Quick-Install-Guide.pdf).

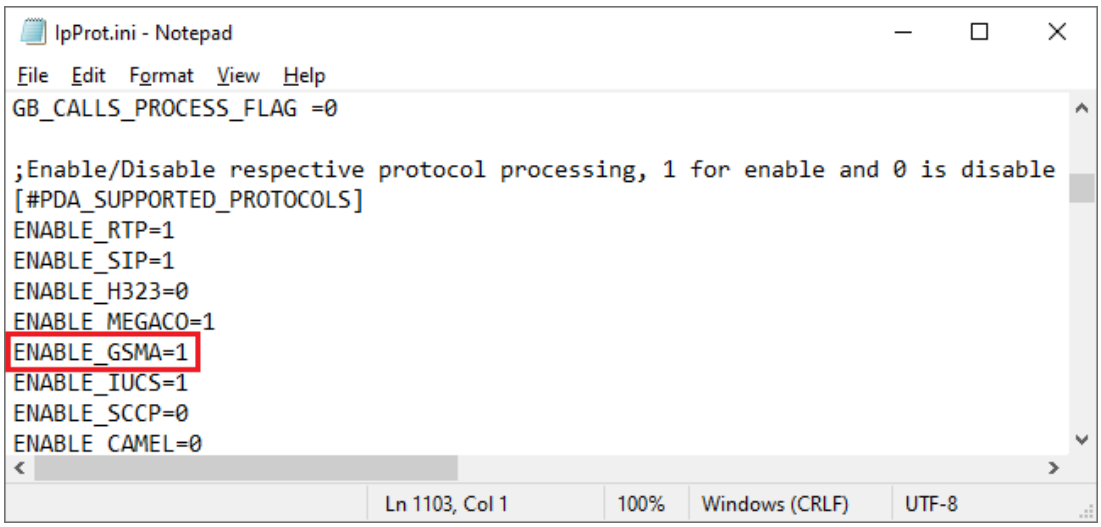
Note: Proceed to the verification steps below after successfully installing the software and verifying the required licenses (PKV100, PKV103) as explained in the Software Quick Installation Guide (Packetscan-Quick-Install-Guide.pdf).

Note:

- Verify that Widows® Firewall is disabled before proceeding with the instructions given below. You should ***Turn off Windows Firewall*** on Windows® and on any 3rd party Anti-Virus software that may be installed on the PC to make sure that Firewall is not blocking any packets or frames.

Pre-Requisite

Users need to configure the **IpProt.ini** file from the following path "**C:\Program Files\GL Communications Inc\PacketScan**". Set the **ENABLE_GSMA** parameter value to '**1**' in the **IPProt.ini**. Save the changes and close the files. Refer to the below screenshot.



Note:

Make sure that the PacketScan™ installation directory has full control permission to save the *.ini files. Follow the below steps to provide writing permission for the **PacketScan** directory.

- Go to " **C:\Program Files\GL Communications Inc**"
- Right click on the "**PacketScan**" folder and select **Properties**
- Click on **Security** tab and click **Edit** from explorer menu
- Click **Add** in the Permission window
- Type '**Everyone**' and click '**Check Names**'. Click **OK** to add this user group to Permissions Window
- Provide full control to the users added and click on **Apply** and **OK**.

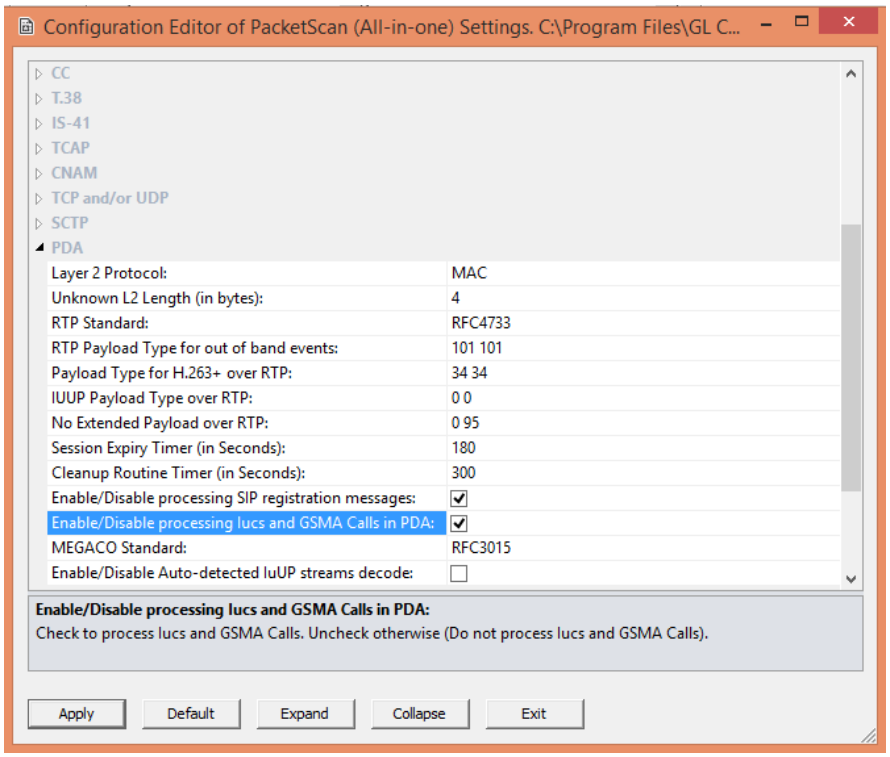
Verification

Follow the steps below for functional verification of **PacketScan™ Real-time** analysis feature.

- Double click on the **PacketScan™** shortcut icon 

created on the desktop to launch the application.

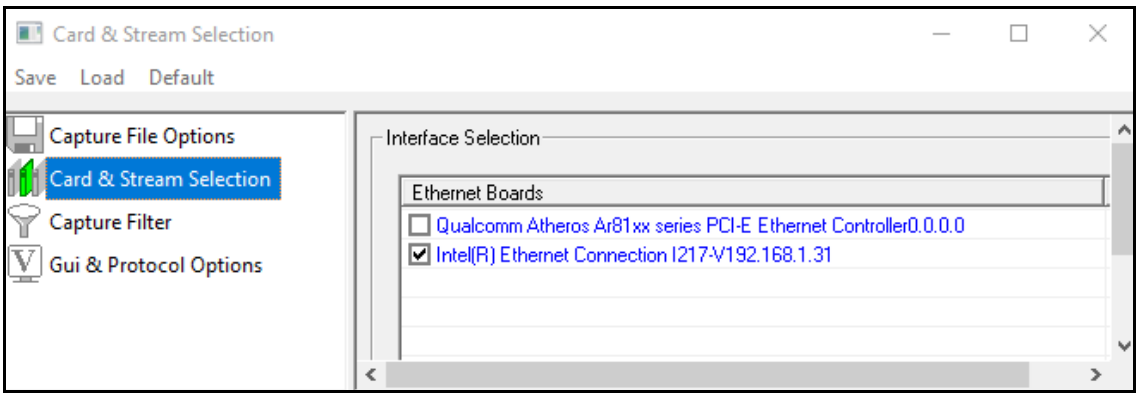
- From the **PacketScan™** main menu, select **Configure → Settings.** This will invoke **Configure Editor of PacketScan Settings window**.
- Check the **Enable/Disable processing IuCS and GSMA Calls in PDA** to enable **IuCS** and **GSMA** calls in PDA. Click on **Apply** and **Exit**. Refer to the below screenshot.



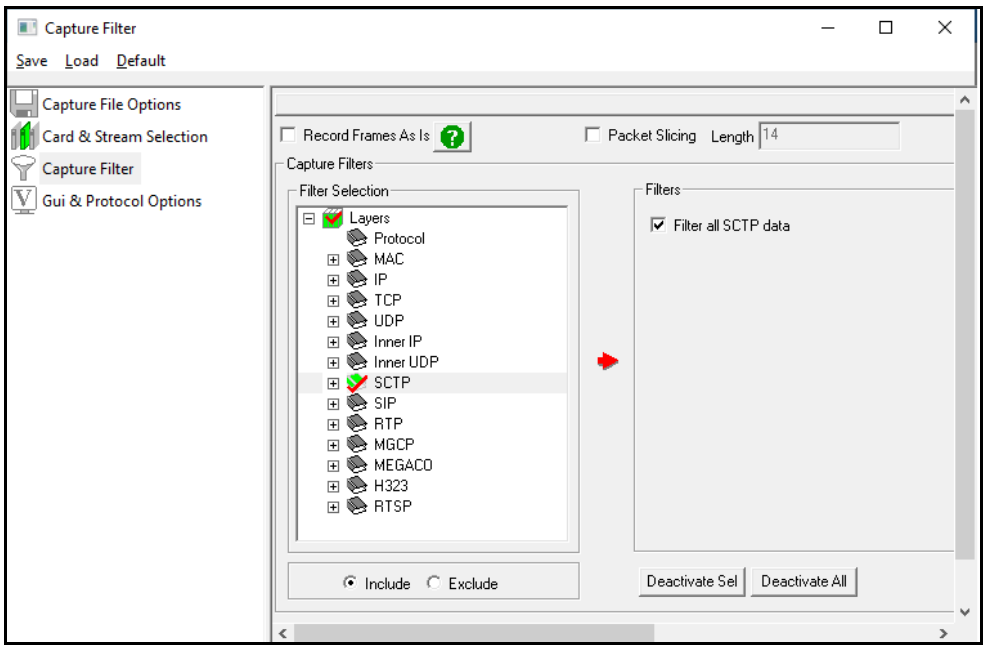
Note:

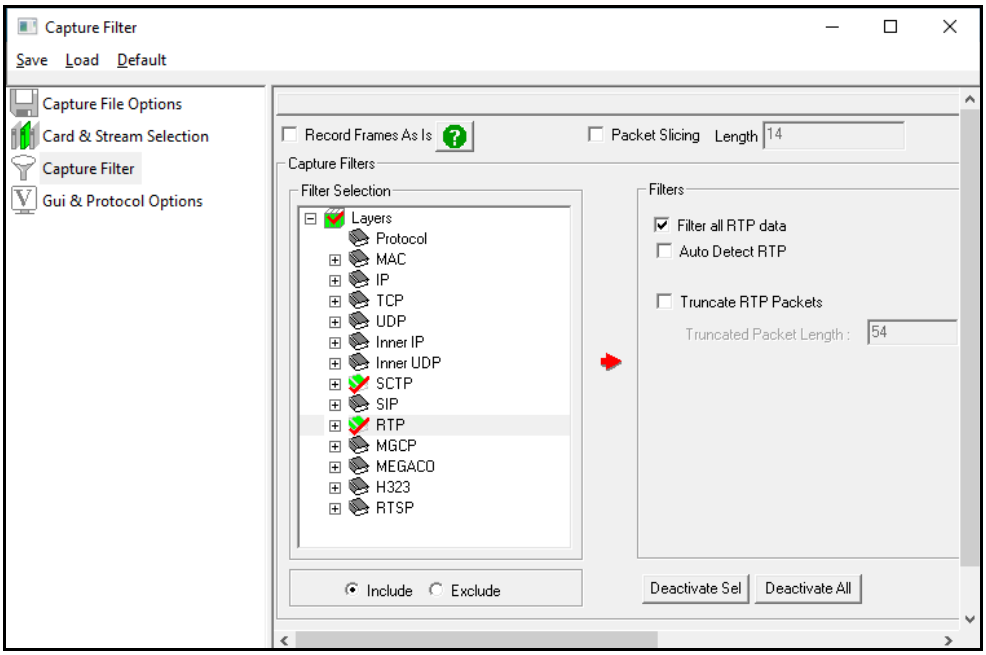
- The values shown here represent generic minimum and maximum values.
- Users can enter the exact minimum and maximum port number range as required. If the user doesn't know the port number, configure minimum and maximum port range as given above.

- A warning message will appear to restart the PacketScan Analyzer. Click on **OK**.
- Close the **PacketScan™** application and invoke again to apply the changes as per configuration settings.
- Select **Capture → Stream/Interface Selection** and enable the Ethernet card on which packet needs to be captured.

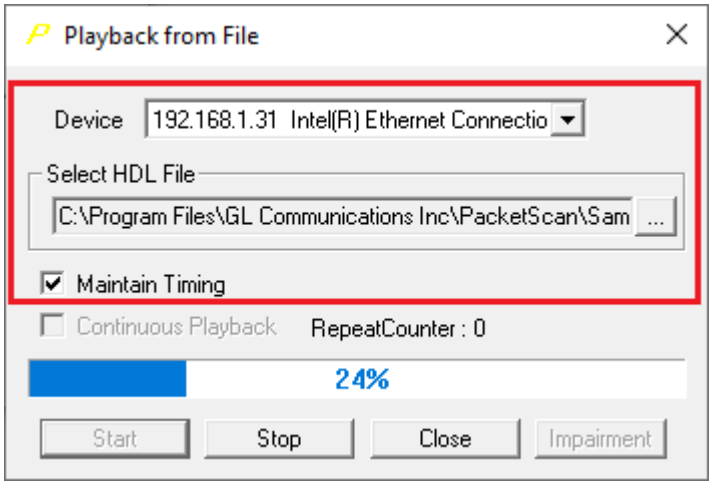


- On the left pane, select **Capture File Options** and verify that **Circular Capture Buffer** is checked.
- Now, on the left pane, select **Capture Filter** option, click **SCTP** in the Filter Selection and check **Filter all SCTP data**. Similarly, click on **RTP** in the Filter Selection, check **Filter all RTP data**. Do not activate any other filters in the **Capture Filter**.

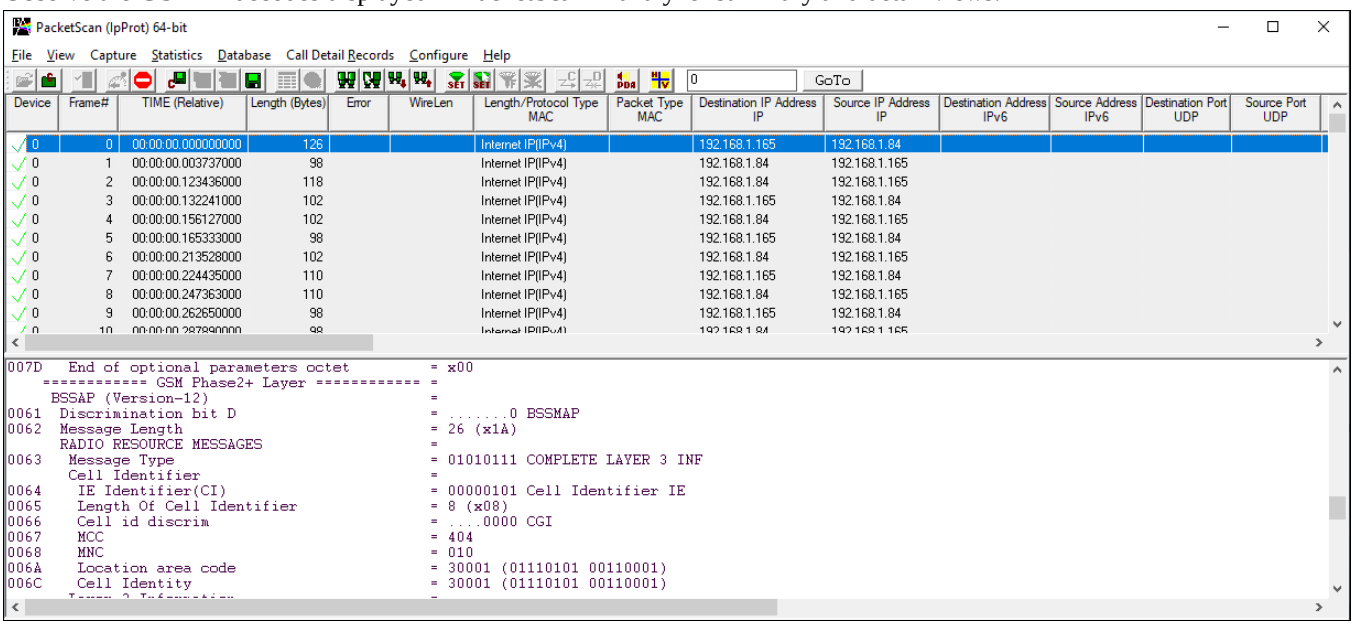




- From the **PacketScan™** main menu, select **File → Start Real-time** or Click **Start Real-time** icon from the toolbar.
- If the **Temp.hdl** file already exists in the PacketScan installation directory, a warning message will appear to replace Temp.hdl file, click **Yes** to overwrite the file.
- Generate traffic by playing HDL file using **PacketscanUtilities** application. From the PacketScan installation directory (**C:\Program Files\GL Communications Inc\PacketScan**) double-click on PacketScanUtilities application. This will invoke PacketScan Utility application.
  - Select **Utilities → HDL Playback** from the menu.
  - In the **Device** option select NIC card on which PacketScan™ Real-time capture is configured. **Note:** Ensure that selected NIC card is enabled in PacketScan™ under **Capture → Stream/Interface Selection**.
  - In the **Select HDL File** option click on browse button to browse and select **C:\Program Files\GL Communications Inc\PacketScan\SampleTraces\GSMAoIP\GSM-A.hdl** file from the PacketScan installation directory
  - Enable **Maintain Timing** option and click **Start**

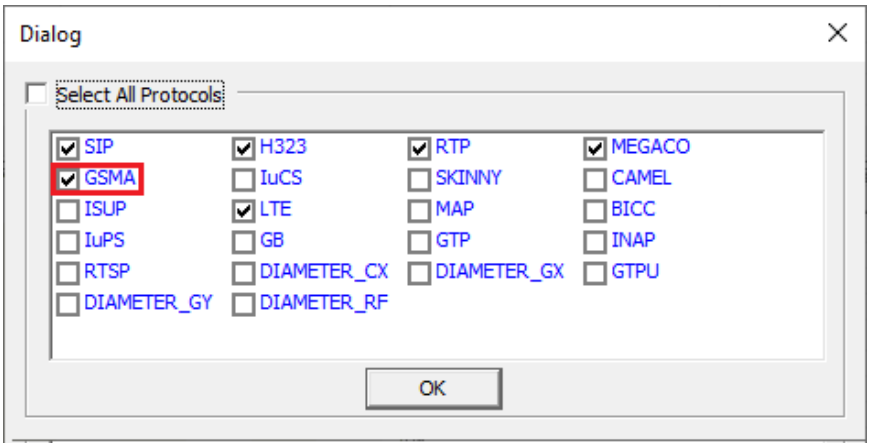


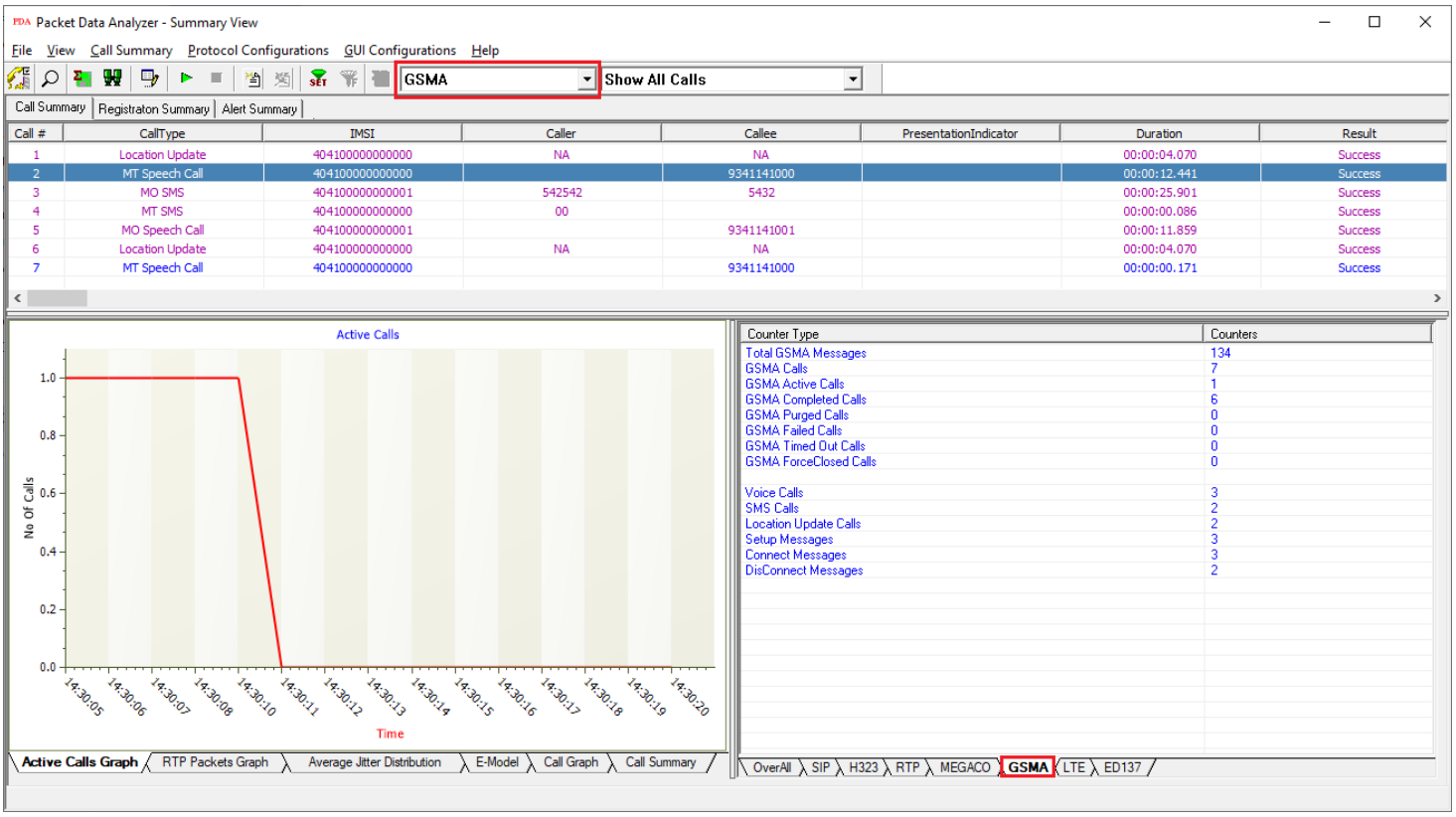
- Observe the **GSM-A** decodes displayed in PacketScan™ analyzer summary and detail views.



- From the **PacketScan™** main toolbar, click on the **PDA**  icon to invoke PDA (Packet Data Analyzer). From the drop-down protocol list select **GSMA**. Select the call in the call summary to view detailed analysis of each session, call graphs and quality scores for the captured **GSMA** calls.

- Select **GUI Configurations → Protocol Statistics Display Configuration** this will display **Dialog** window. Check the **GSMA** option to view the **GSMA** counters on PDA. Refer to the below screenshots.





Note:

- You should ***Turn off Windows Firewall*** on Windows® and on any 3rd party Anti-Virus software that may be installed on the PC to make sure that Firewall is not blocking any packets or frames.