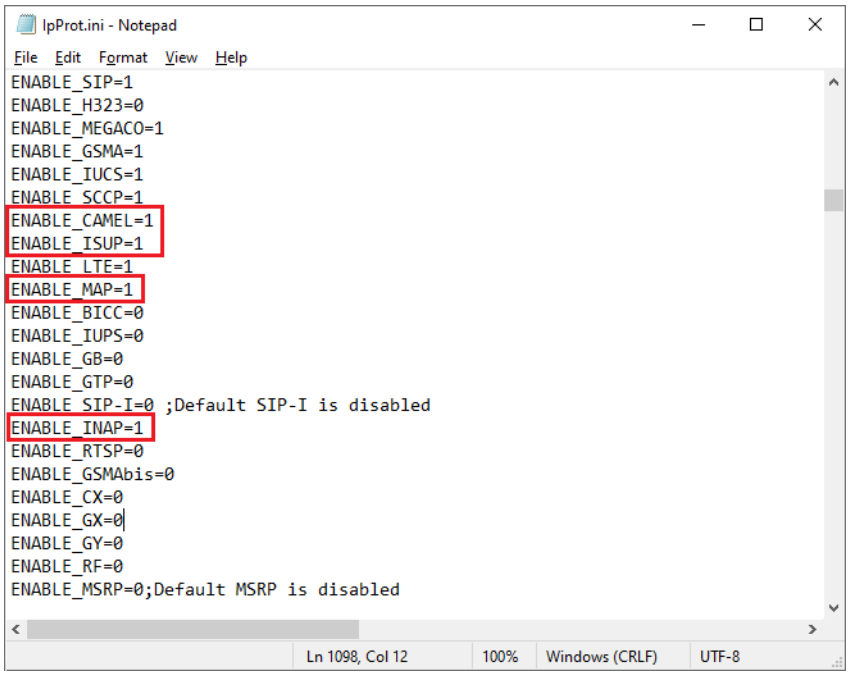
It is assumed that the PacketScan™ Analyzer Software and License installations (PKV100, PKV105) are already performed referring to the Software Quick Installation Guide (Packetscan-Quick-Install-Guide.pdf). Now proceed with the verification steps below for capturing and analyzing SIGTRAN protocol.

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.
- PacketScan™ SIGTRAN protocol does not support Packet Data Analysis.

Verification

- To make sure that **SIGTRAN** protocols are enabled, user need to update **IpProt.ini** file.
- Navigate to PacketScan™ Installation directory **C:\Program Files\GL Communications Inc\PacketScan** and look for **IpProt.ini** file and open with notepad.
- Set values for the parameters **ENABLE_ISUP, ENABLE_CAMEL, ENABLE_MAP, ENABLE_INAP** as **1** (1 to enable & 0 to disable) For example: ENABLE_ISUP=1, ENABLE_CAMEL=1, ENABLE_MAP=1, ENABLE_INAP=1
- Save and exit the file.

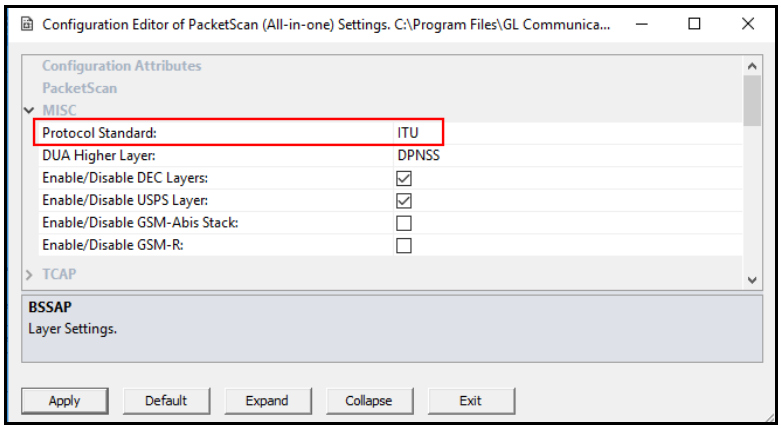


- Double click on the **PacketScan™** shortcut icon 

created on the desktop to launch the application.

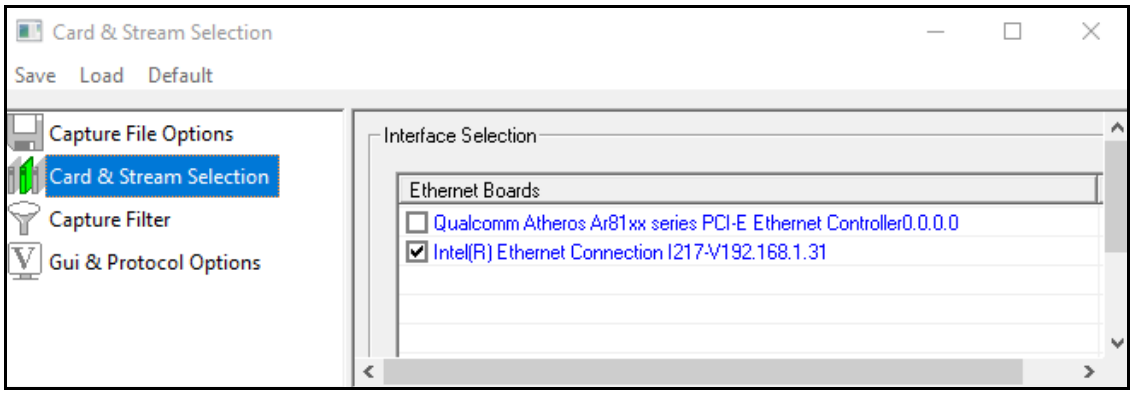
Follow the steps below for functional verification of PacketScan™ **Real-time** analysis feature.

- From the **PacketScan™** main menu, select **Configure → Settings.** This will invoke **Configure Editor of PacketScan Settings** window.
- Expand **MISC** option, select **Protocol Standard** as **ITU** from drop-down list. User can also select **ANSI** or **ETSI Protocol Standards** as required. Click on **Apply** and **Exit**. Refer to the below screenshot.

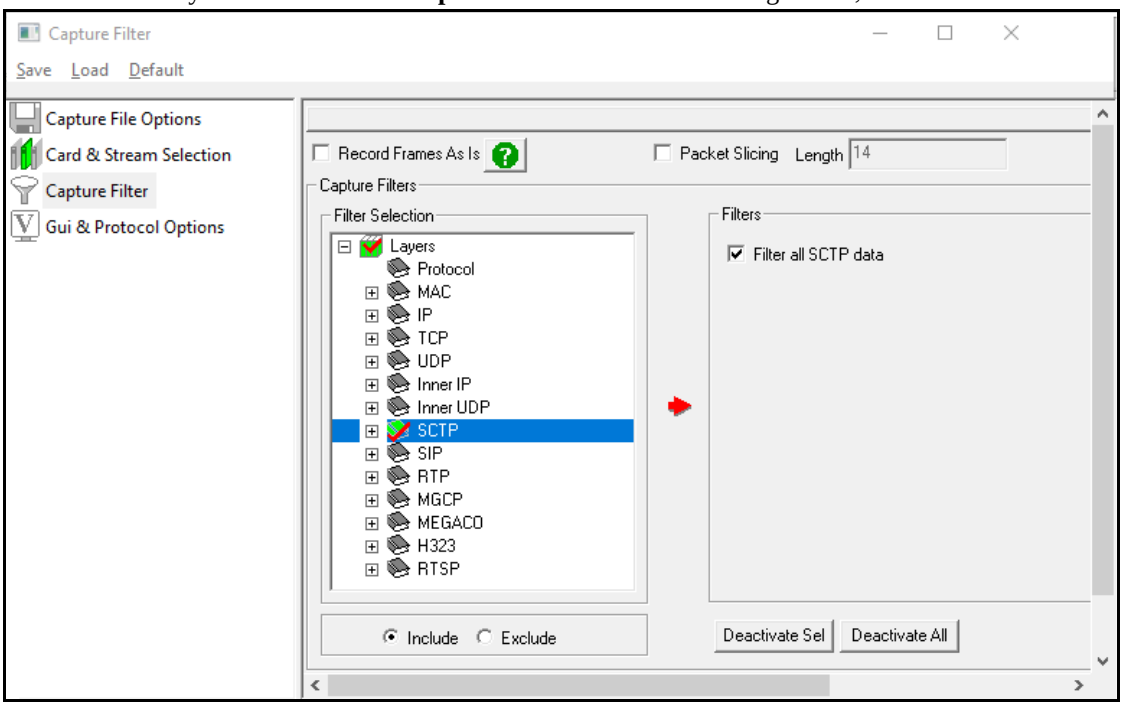


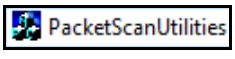
- A warning message will appear to restart the PacketScan Analyzer. Click on **OK**.
- Close the **PacketScan™** application and invoke again to apply the changes as per configuration settings.

- Select **Capture → Stream/Interface Selection** and enable the Ethernet card on which packet needs to be captured.



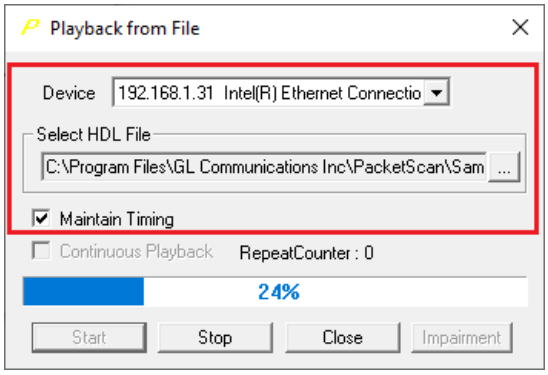
- On the left pane, select **Capture File Options** and verify that **Circular Capture Buffer** is checked.
- Now, on the left pane, select **Capture Filter** option, click **SCTP** in the Filter Selection and check **Filter all SCTP data**. Do not activate any other filters in the **Capture Filter**.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



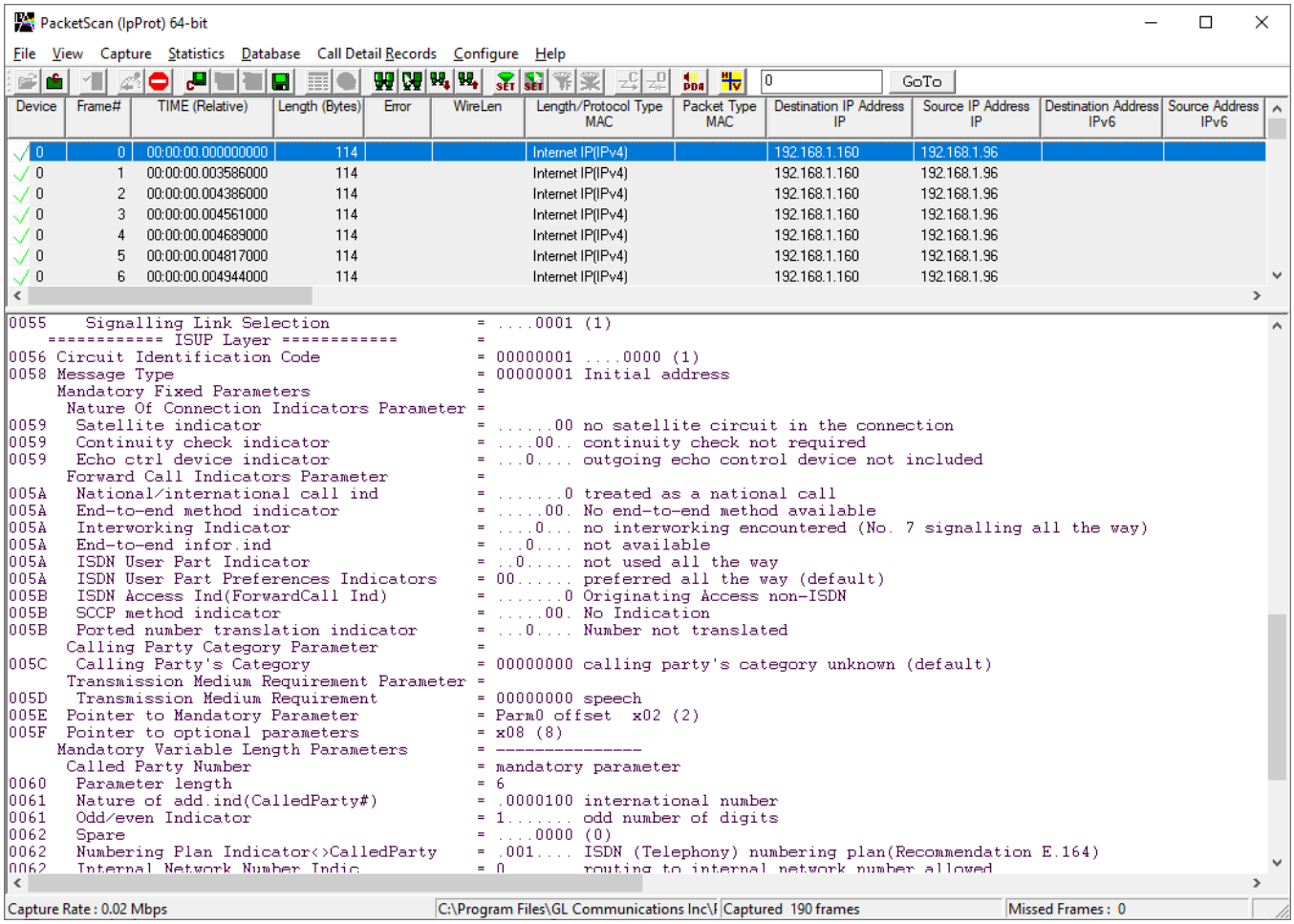
- From the **PacketScan™** main menu, select **File → Start Real-time** or Click **Start Real-time**  icon from the toolbar.
- If the Temp.hdl file already exists in the PacketScan installation directory, a warning message will appear to replace Temp.hdl file, click **Yes** to overwrite the file.
- Generate traffic by playing HDL file using PacketscanUtilities application. From the PacketScan installation directory (**C:\Program Files\GL Communications Inc\PacketScan**) double-click on 

application. This will invoke **PacketScan Utility** application.

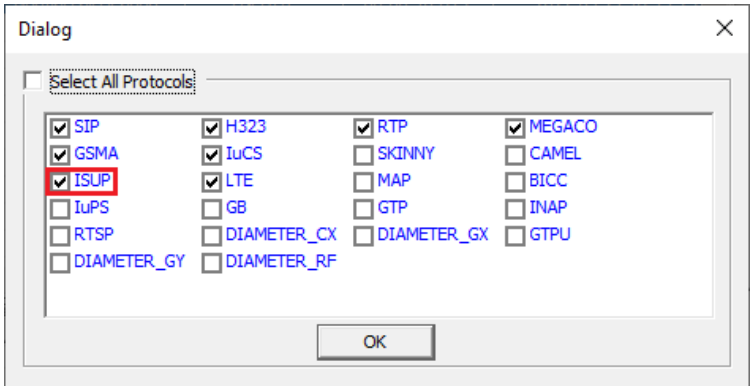
- Select **Utilities → HDL Playback** from the menu.
- In the **Device** option select NIC card on which PacketScan™ Real-time capture is configured. **Note:** Ensure that selected NIC card is enabled in PacketScan™ under **Capture → Stream/Interface Selection**.
- In the **Select HDL File** option click on browse button to browse and select **C:\Program Files\GL Communications Inc\PacketScan\SampleTraces\Sigtran\ISUP_Sigtran_ITU.hdl** file from the PacketScan installation directory.
- Enable **Maintain Timing** option and click **Start**.

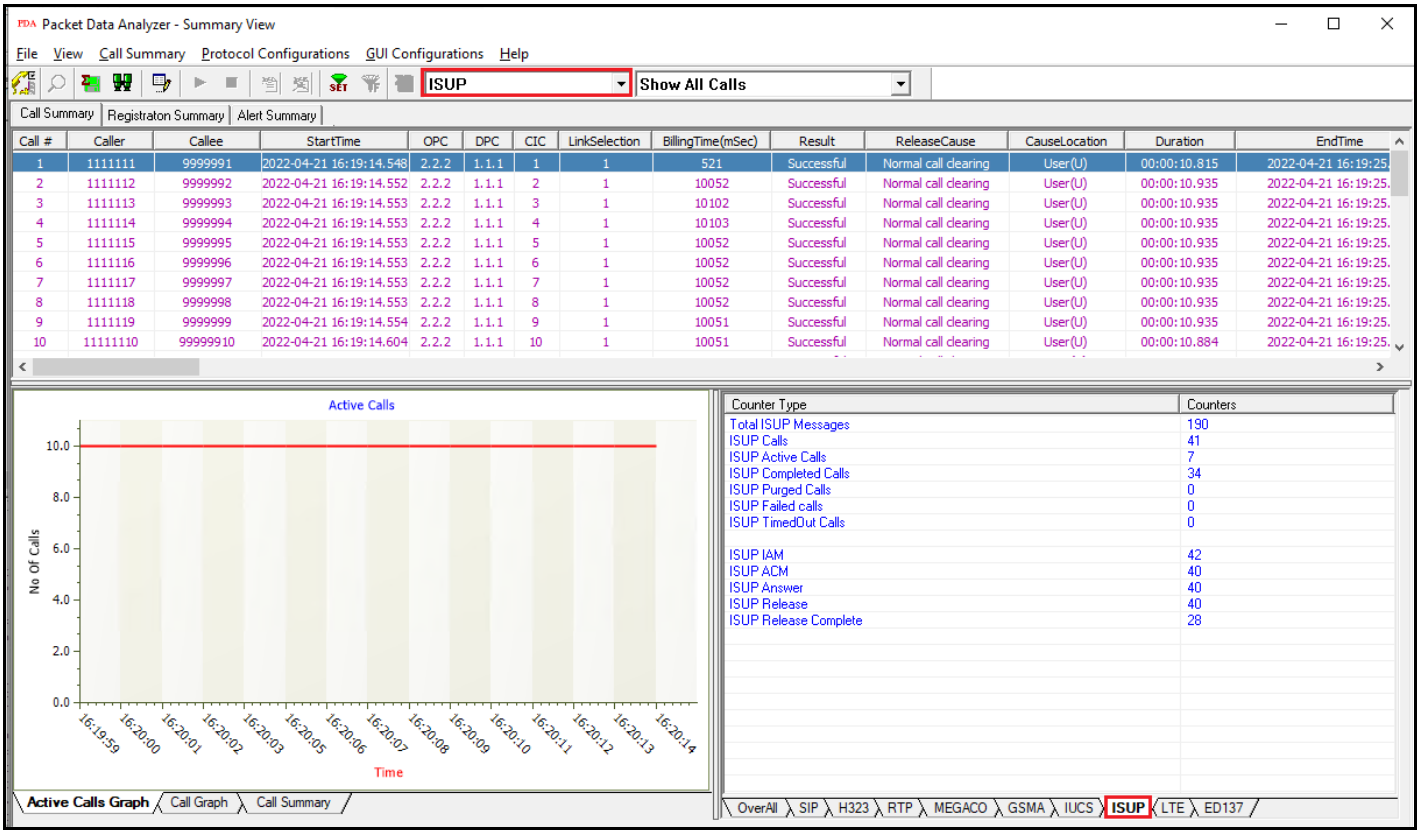


- Observe the **ISUP SIGTRAN** decodes displayed in PacketScan™ analyzer summary and detail views.



- From the **PacketScan™** main toolbar, click on the **PDA** icon to invoke PDA (Packet Data Analyzer), from the drop-down protocol list select **ISUP** to view detail analysis of each session, call graphs and quality scores for the captured **ISUP** Traffic.
- Select **GUI Configurations → Protocol Statistics Display Configuration** this will display **Dialog** window. Check the **ISUP** option to view the **ISUP** 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.