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, PKV104) as explained in the Software Quick Installation Guide (Packetscan-Quick-Install-Guide.pdf).

Verification

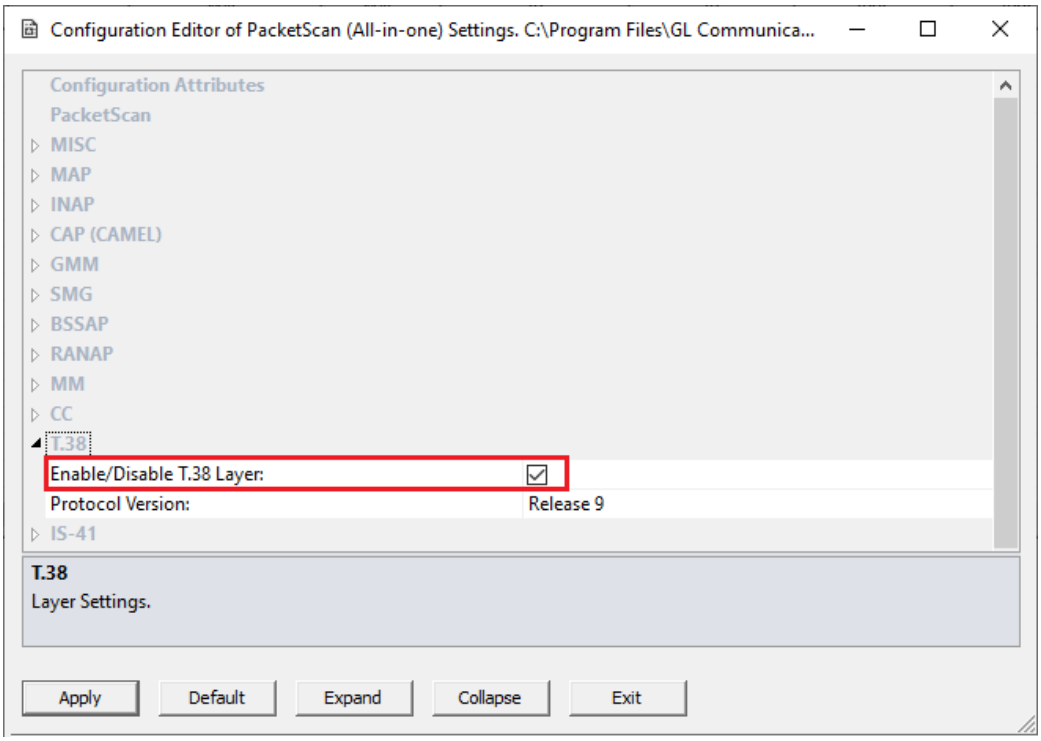
Follow the steps below for functional verification of PacketScan™ **Real-time** analysis feature.

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

created on the desktop to launch the application

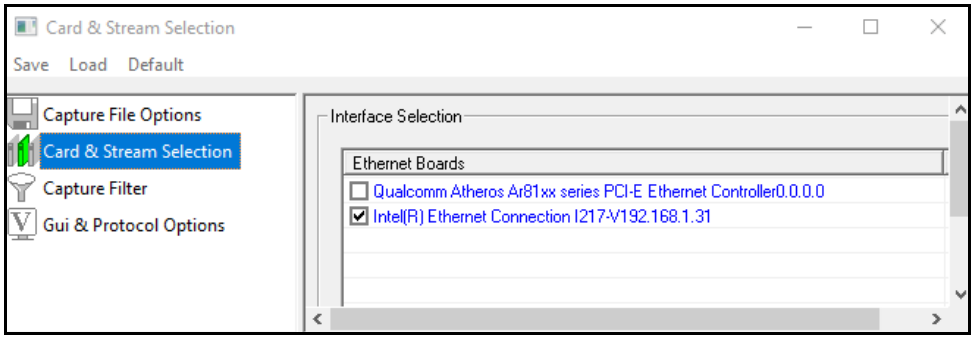
Follow the steps below for functional verification of PacketScan™ **Real-time** analysis feature.

- From the **PacketScan™** main menu, select **Configure → Settings**. This will invoke **Configure Editor** of PacketScan Settings window.
- Expand **T.38** option, check **Enable/Disable T.38 Layer** option. Click on **Apply** and **Exit**. Refer to the below screenshot.

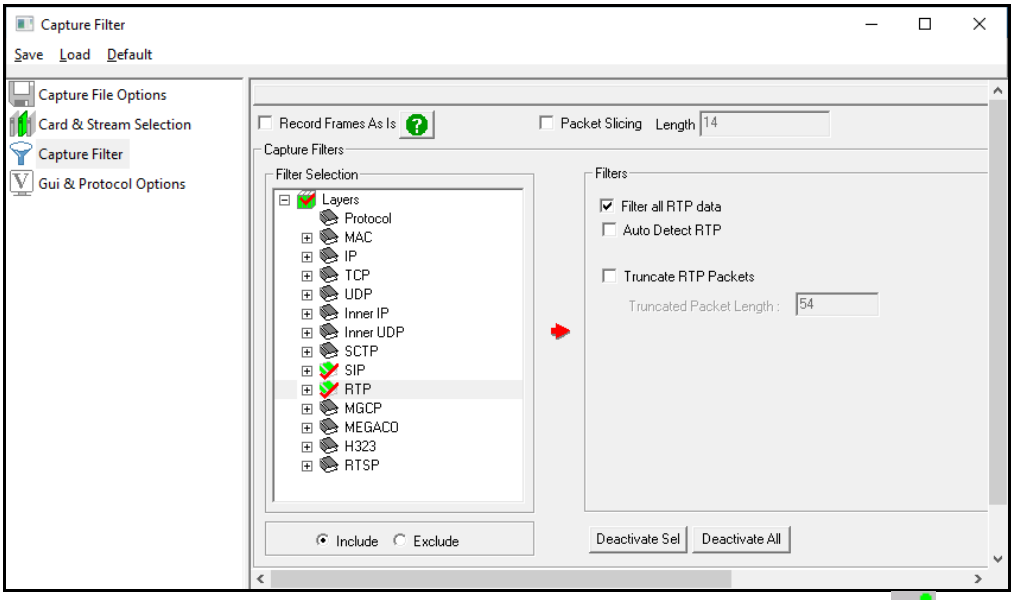


- A warning message will appear to restart the PacketScan™ Analyzer. Click on **OK**.
- Close the **PacketScan™** application and invoke again to apply the changes as per configuration settings.

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

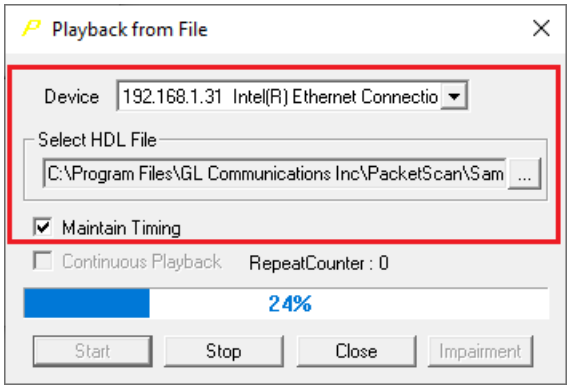


- On the left pane, select **Capture → Capture File Options** and enable **Circular Capture Buffer**
- Now, on the left pane, select **Capture → Capture Filter** option, click **SIP** in the Filter Selection and check **Filter all SIP data**. Do not activate any other filters in the **Capture Filter**. Similarly, click **RTP** in the Filter Selection and check **Filter all RTP data** and **Auto Detect RTP** options. Close the window.

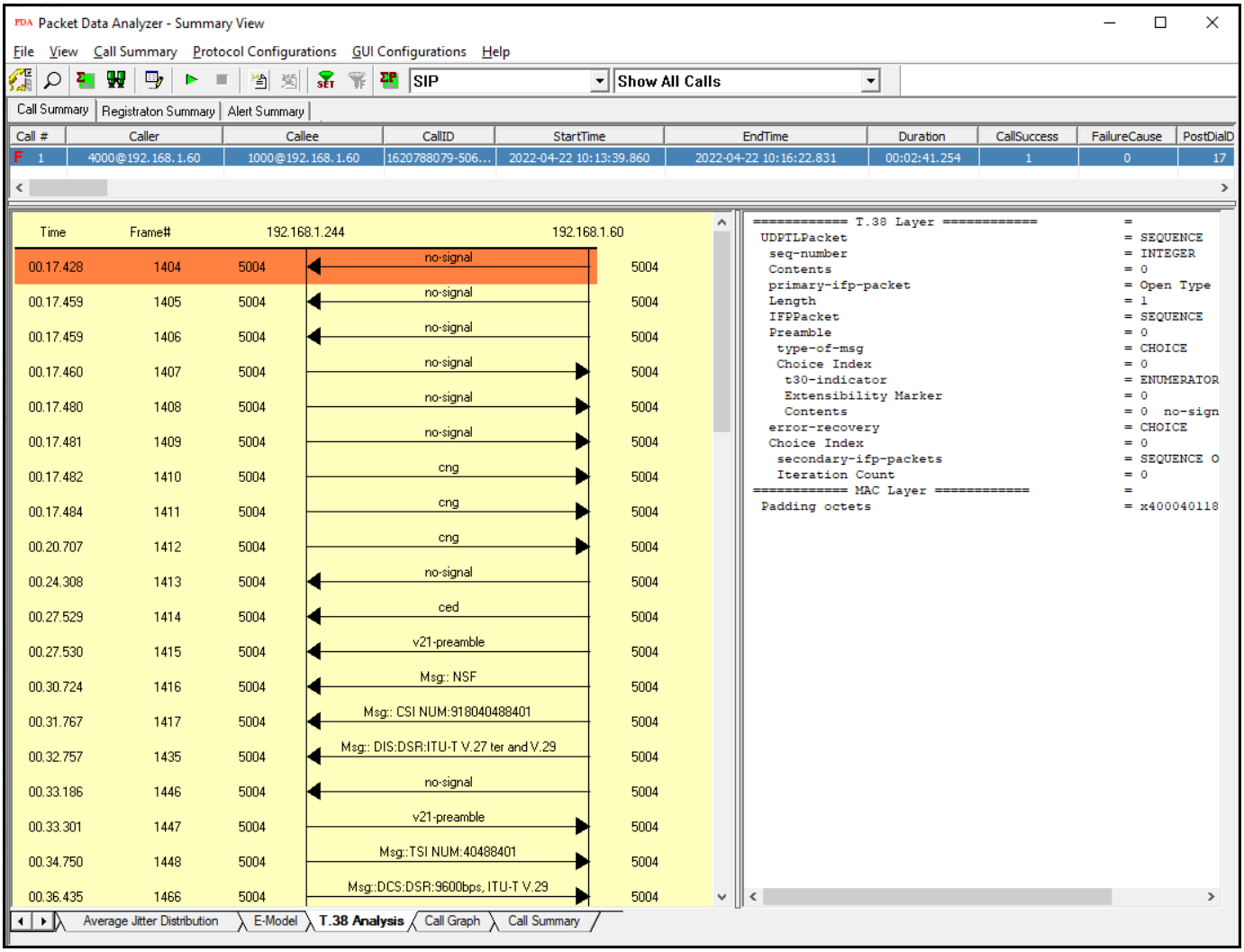


- From the **PacketScan™** main menu, select **File → Start Real-time** or Click **Start Real-time** icon from the toolbar.
- If the **Temp.hdl** file already exists in the PacketScan installation directory, a warning message will appear to replace Temp.hdl file, click **Yes** to overwrite the file.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

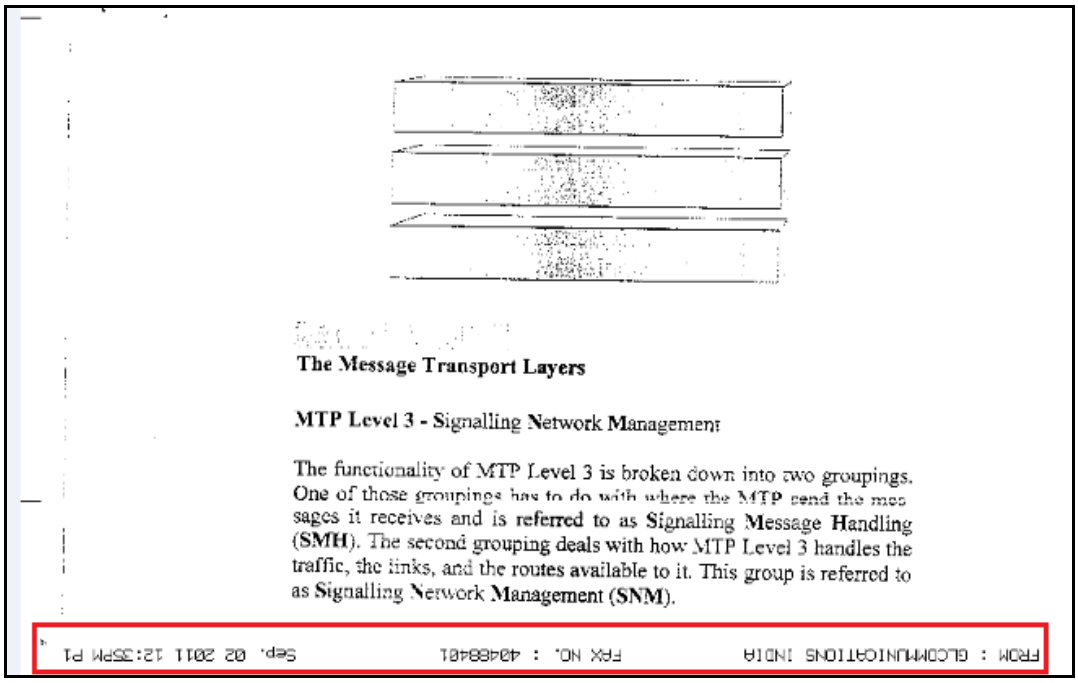
- In the **Select HDL File** option click on browse button to browse and select **C:\Program Files\GL Communications Inc\PacketScan\SampleTraces\SIP\FAX.hdl** file from the PacketScan installation directory.
- Enable **Maintain Timing** option and click **Start**.



- From the **PacketScan™** main toolbar, click on the PDA icon to invoke PDA (Packet Data Analyzer) and view detail analysis of each fax session**, call graphs**, **T38 analysis graph**, and **quality scores** for the captured fax calls.



- In PDA, select **Call Summary → Extract Fax Image**, in the **Extract Fax Image from Call** window, select **CallNum_1** from the left pane and click on **Right arrow** to move the call into right pane.
- Now, in the Path option click on browse button and select the required path.
- Click on **Extract image.** Navigate to the destination folder and verify the extracted image (Tiff file) as shown below.



The Message Transport Layers

MTP Level 3 - Signalling Network Management

The functionality of MTP Level 3 is broken down into two groupings. One of those groupings has to do with where the MTP send the messages it receives and is referred to as Signalling Message Handling (SMH). The second grouping deals with how MTP Level 3 handles the traffic, the links, and the routes available to it. This group is referred to as Signalling Network Management (SNM).

FROM : GLCOMMUNICATIONS INDIA FAX NO. : 4048840 Sep. 02 2011 12:35PM P1

Note: If you are unable to view the real-time decodes, verify if the Widows® Firewall is enabled. 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.