

*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](#)).*

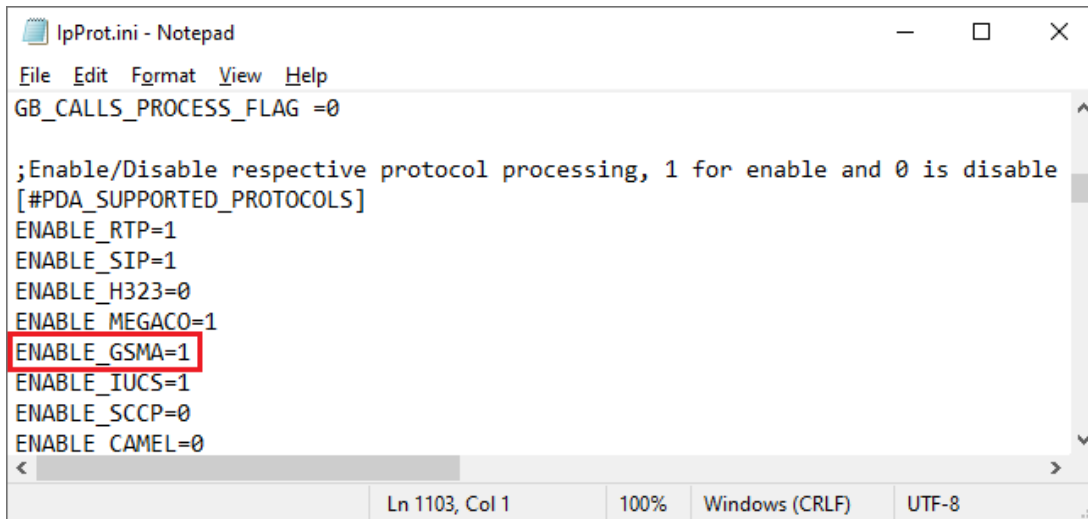


**Note:**

- Verify that Windows® Firewall is disabled before proceeding with the instructions given below. You should **Turn off Windows Firewall** on Windows® and on any 3<sup>rd</sup> 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.



The screenshot shows a Notepad window titled "IpProt.ini - Notepad". The menu bar includes File, Edit, Format, View, and Help. The text content of the file is as follows:

```
GB_CALLS_PROCESS_FLAG =0

;Enable/Disable respective protocol processing, 1 for enable and 0 is disable
[#PDA_SUPPORTED_PROTOCOLS]
ENABLE_RTP=1
ENABLE_SIP=1
ENABLE_H323=0
ENABLE_MEGACO=1
ENABLE_GSMA=1
ENABLE_IUCS=1
ENABLE_SCCP=0
ENABLE_CAMEL=0
```

The line **ENABLE\_GSMA=1** is highlighted with a red rectangular box. The status bar at the bottom indicates "Ln 1103, Col 1", "100%", "Windows (CRLF)", and "UTF-8".



**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**.

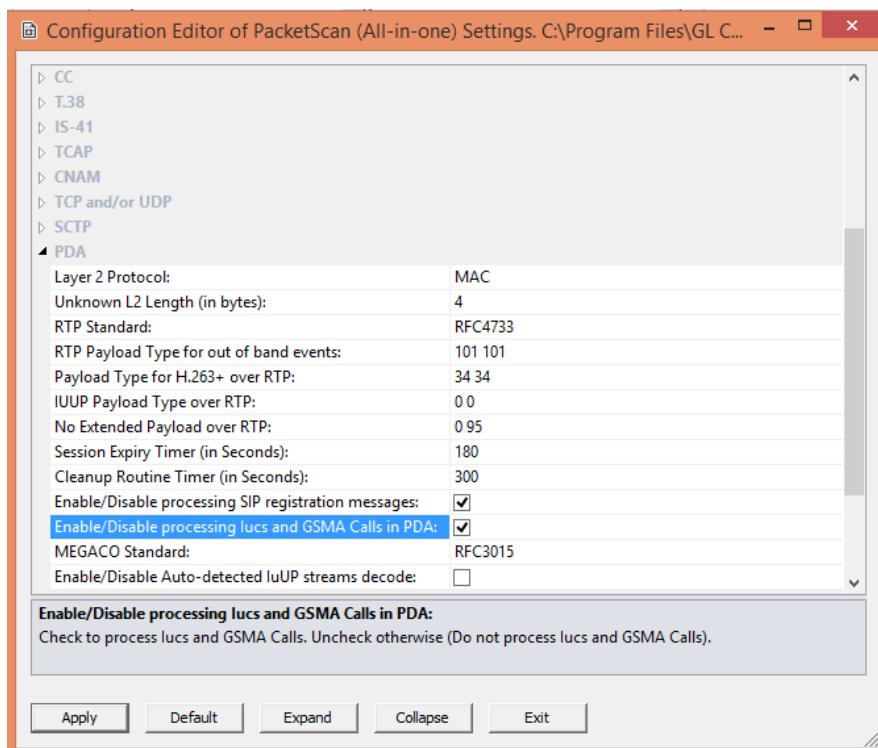


### Verification

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

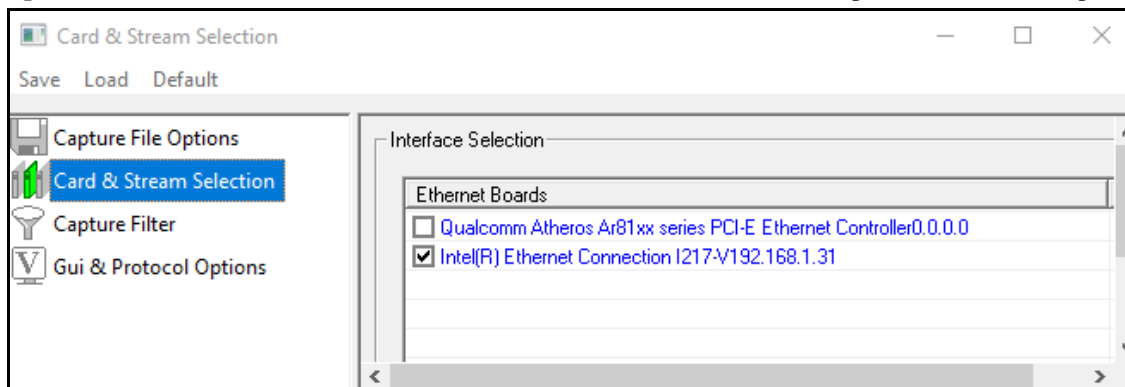


- Double click on the **PacketScan™** shortcut icon created on the desktop to launch the application.
- From the **PacketScan™** main menu, select **Configure → Settings**. This will invoke **Configure Editor of PacketScan Settings window**.
- Check the **Enable/Disable processing luCS and GSMA Calls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

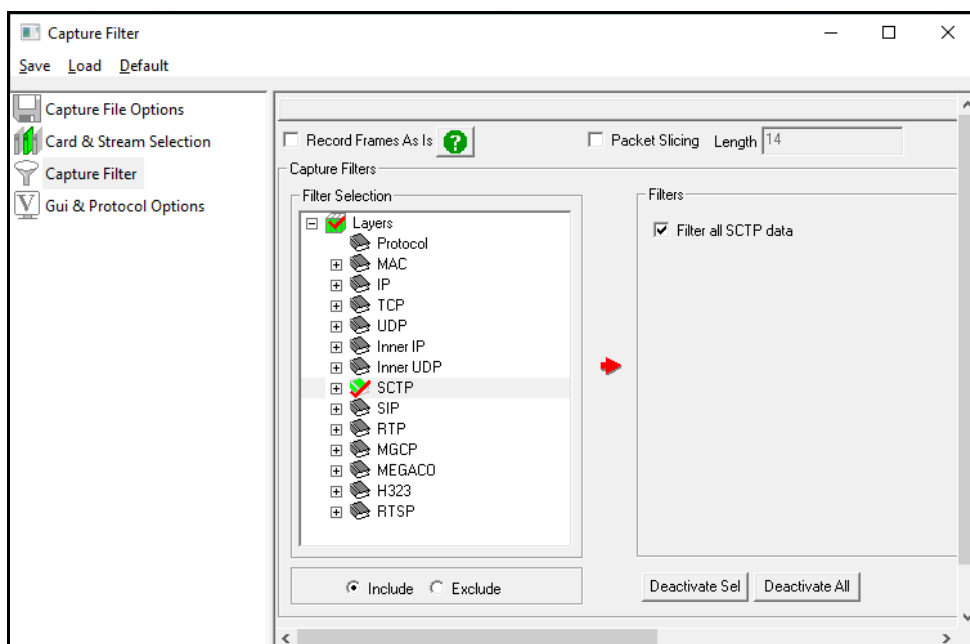


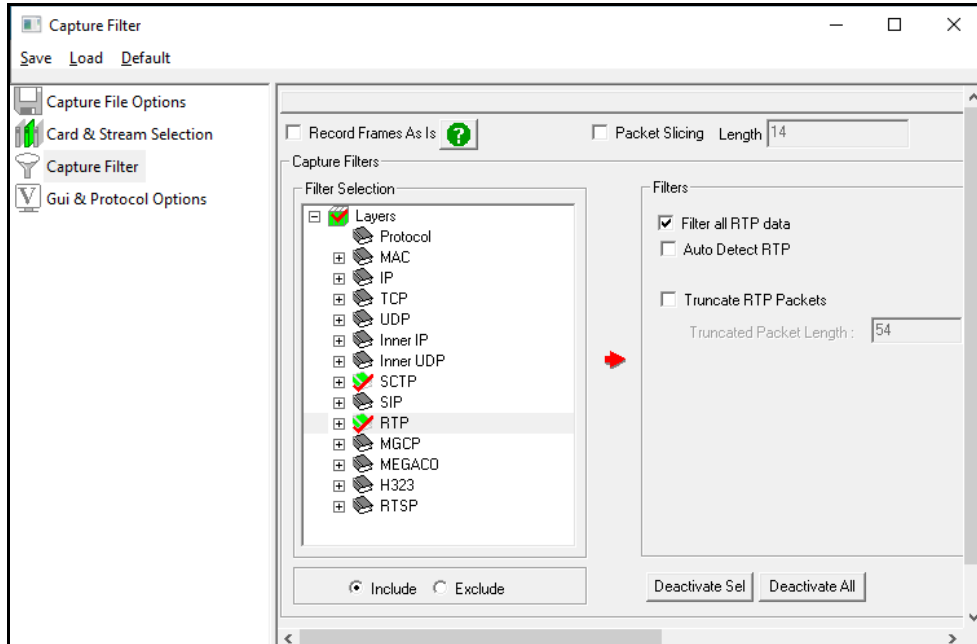
- Note:**
- The values shown here represent generic minimum and maximum values.
  - Users can enter the exact minimum and maximum port number range as required. If the user doesn't know the port number, configure minimum and maximum port range as given above.



- 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.

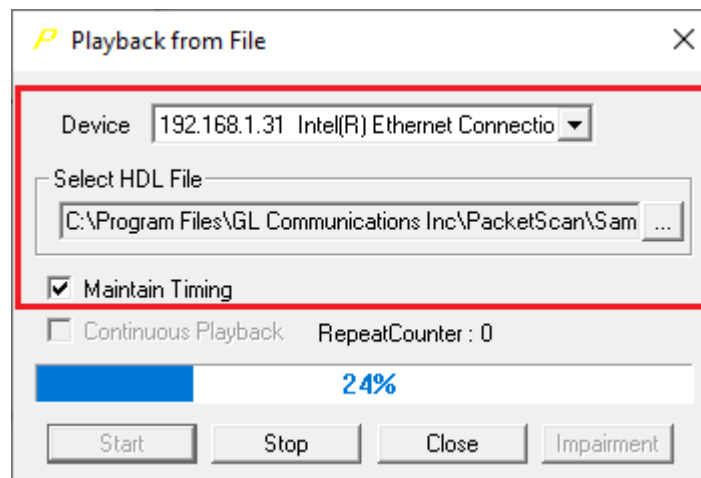


- On the left pane, select **Capture File Options** and verify that **Circular Capture Buffer** is checked.
- Now, on the left pane, select **Capture Filter** option, click **SCTP** in the Filter Selection and check **Filter all SCTP data**. Similarly, click on **RTP** in the Filter Selection, check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

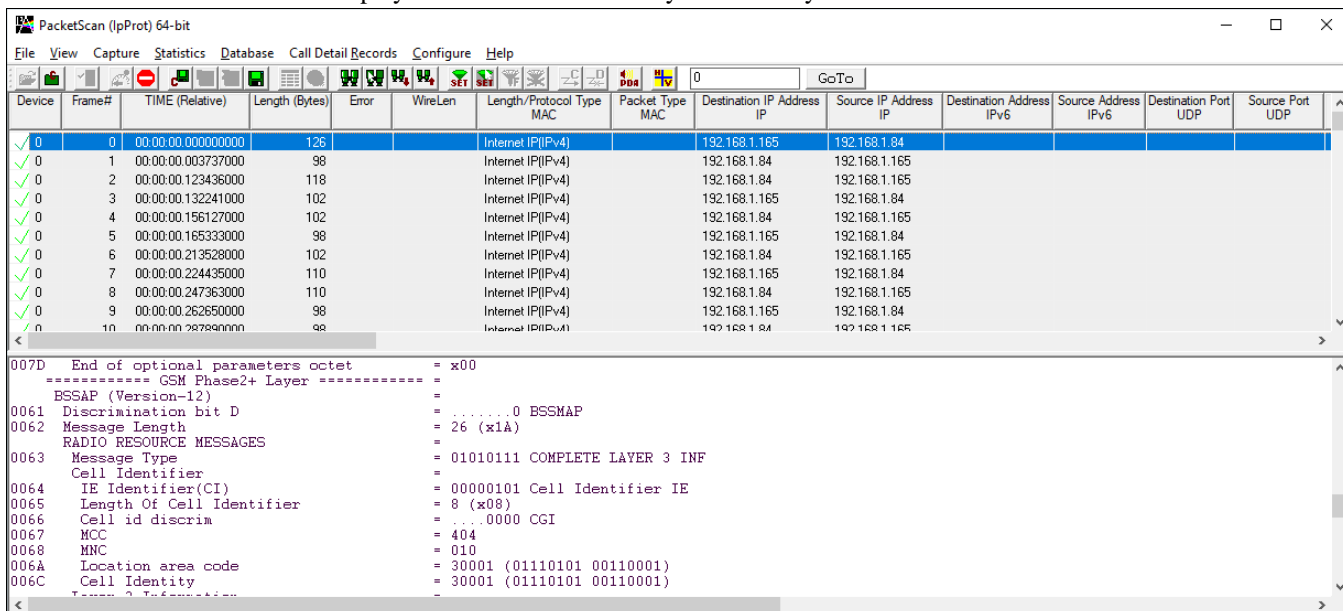




- From the **PacketScan™** main menu, select **File → Start Real-time** or Click **Start Real-time**  icon from the toolbar.
- If the **Temp.hdl** file already exists in the PacketScan installation directory, a warning message will appear to replace Temp.hdl file, click **Yes** to overwrite the file.
- 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.




Device	Frame#	TIME (Relative)	Length (Bytes)	Error	WireLen	Length/Protocol Type	Packet Type	Destination IP Address	Source IP Address	Destination Address	Source Address	Destination Port	Source Port
✓ 0	0	00:00:00.000000000	126			Internet IP(IPv4)		192.168.1.165	192.168.1.84				
✓ 0	1	00:00:00.003737000	98			Internet IP(IPv4)		192.168.1.84	192.168.1.165				
✓ 0	2	00:00:00.123436000	118			Internet IP(IPv4)		192.168.1.84	192.168.1.165				
✓ 0	3	00:00:00.132241000	102			Internet IP(IPv4)		192.168.1.165	192.168.1.84				
✓ 0	4	00:00:00.156127000	102			Internet IP(IPv4)		192.168.1.84	192.168.1.165				
✓ 0	5	00:00:00.165333000	98			Internet IP(IPv4)		192.168.1.165	192.168.1.84				
✓ 0	6	00:00:00.213528000	102			Internet IP(IPv4)		192.168.1.84	192.168.1.165				
✓ 0	7	00:00:00.224435000	110			Internet IP(IPv4)		192.168.1.165	192.168.1.84				
✓ 0	8	00:00:00.247363000	110			Internet IP(IPv4)		192.168.1.84	192.168.1.165				
✓ 0	9	00:00:00.262650000	98			Internet IP(IPv4)		192.168.1.165	192.168.1.84				
✓ 0	10	00:00:00.287990000	98			Internet IP(IPv4)		192.168.1.84	192.168.1.165				

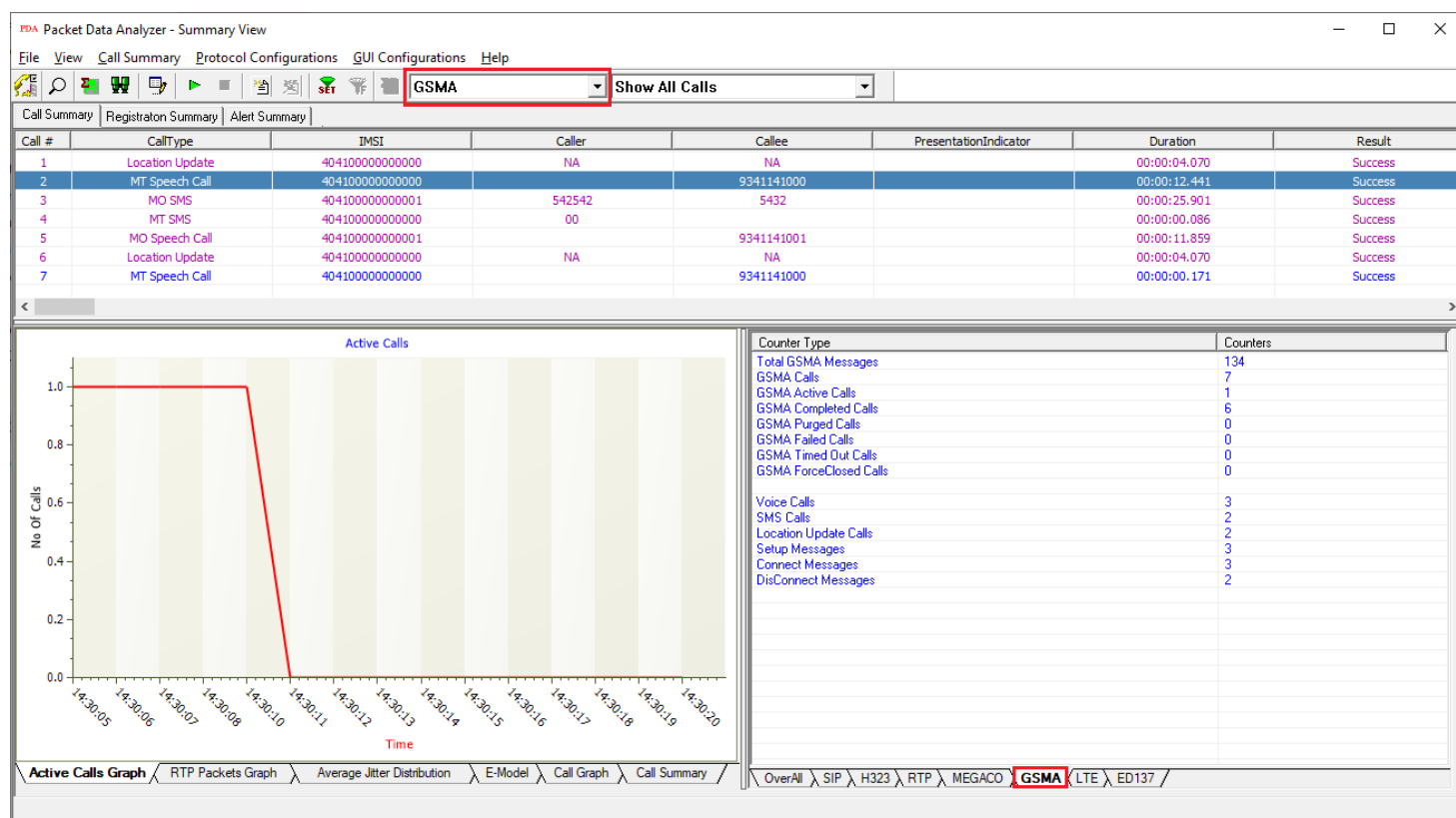
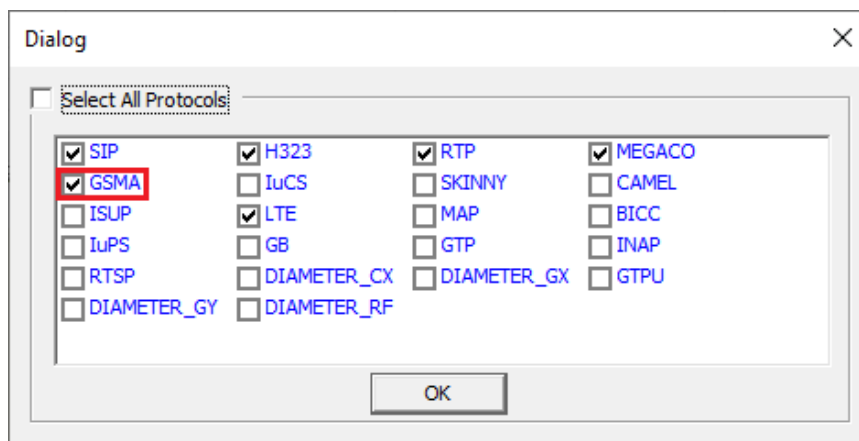
  

```

007D End of optional parameters octet = x00
===== GSM Phase2+ Layer =====
BSSAP (Version-12)
0061 Discrimination bit D = .....0 BSSMAP
0062 Message Length = 26 (x1A)
RADIO RESOURCE MESSAGES
0063 Message Type = 01010111 COMPLETE LAYER 3 INF
Cell Identifier
0064 IE Identifier(CI) = 00000101 Cell Identifier IE
0065 Length Of Cell Identifier = 8 (x08)
0066 Cell id discrim = ....0000 CGI
0067 MCC = 404
0068 MNC = 010
006A Location area code = 30001 (01110101 00110001)
006C Cell Identity = 30001 (01110101 00110001)
  
```

- 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.