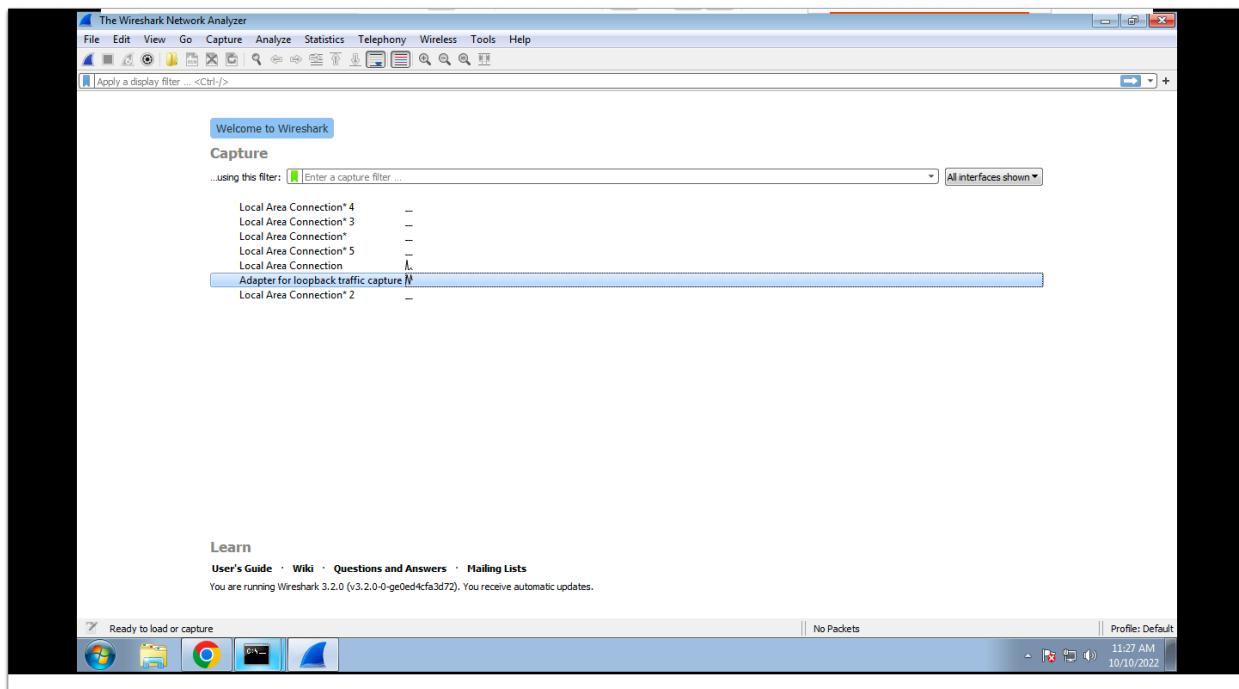


Observation on ports by ScadaBR.exe

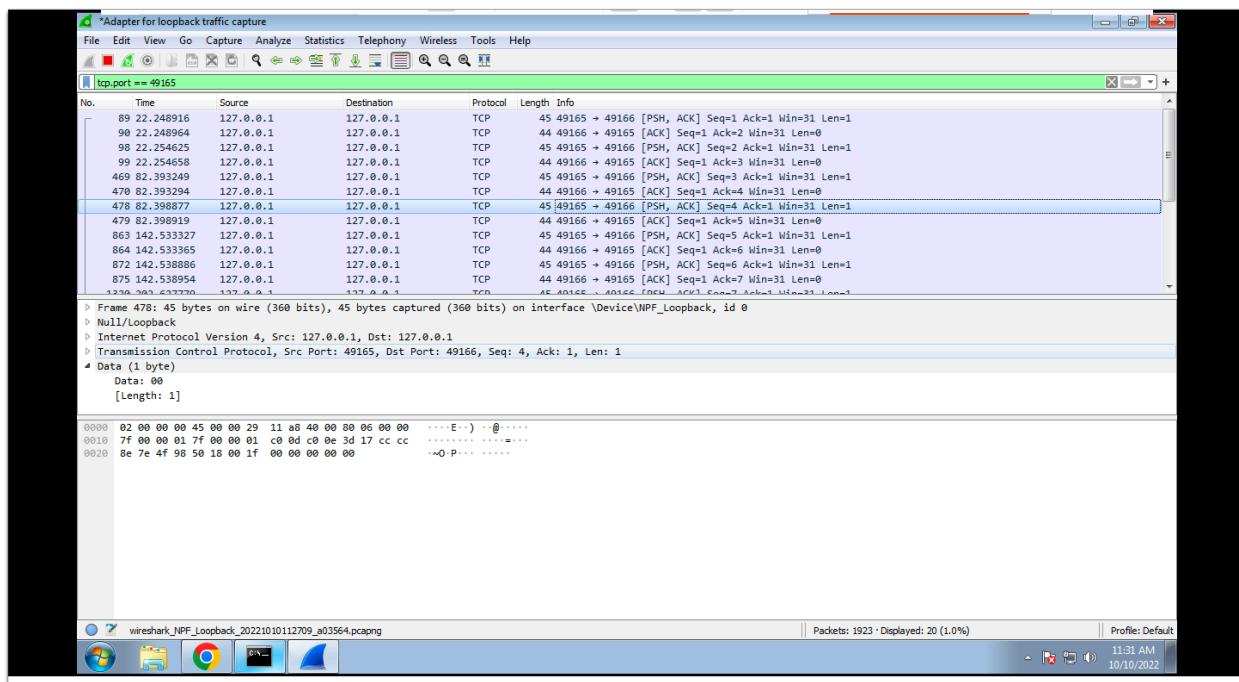
I did research with both Wireshark and Nmap.

Select the loopback interface to fetch traffic sending to host itself.

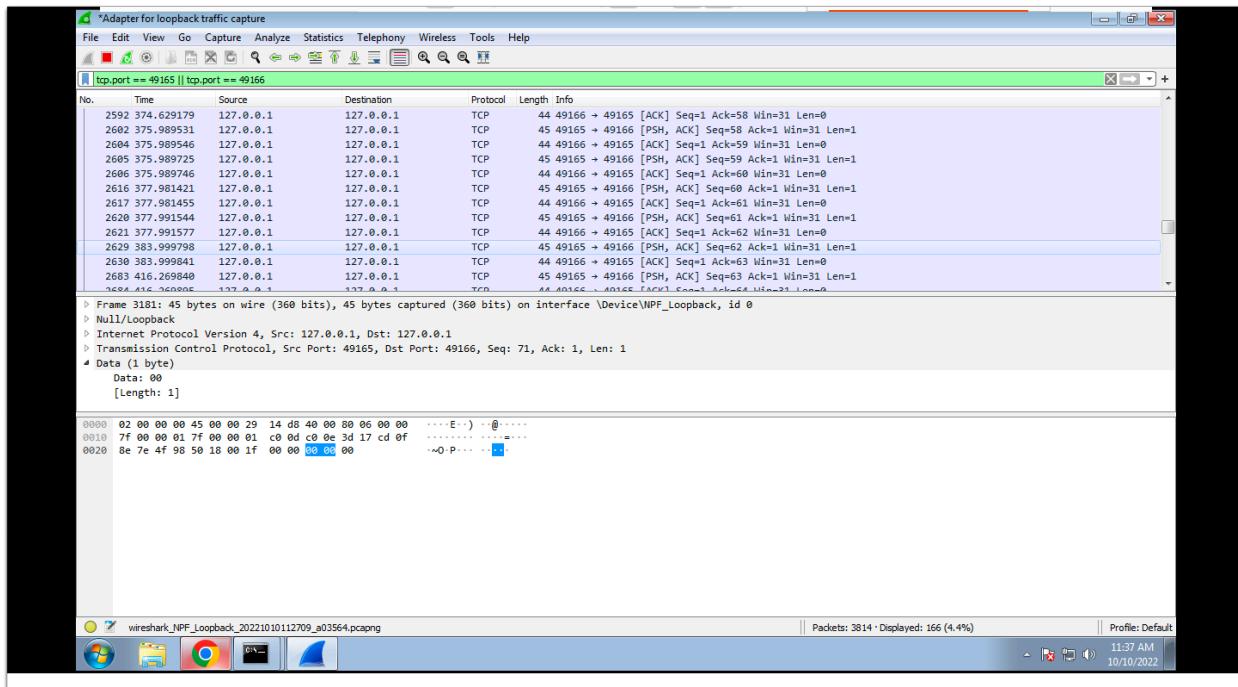
The traffic is saved as attachment “ScadaBR_port_49165_49166_traffic.pcapng”



From the observation, I found that the lower value port is always sending Data 0 to the higher port, even if I did some interaction with ScadaBR web interface.

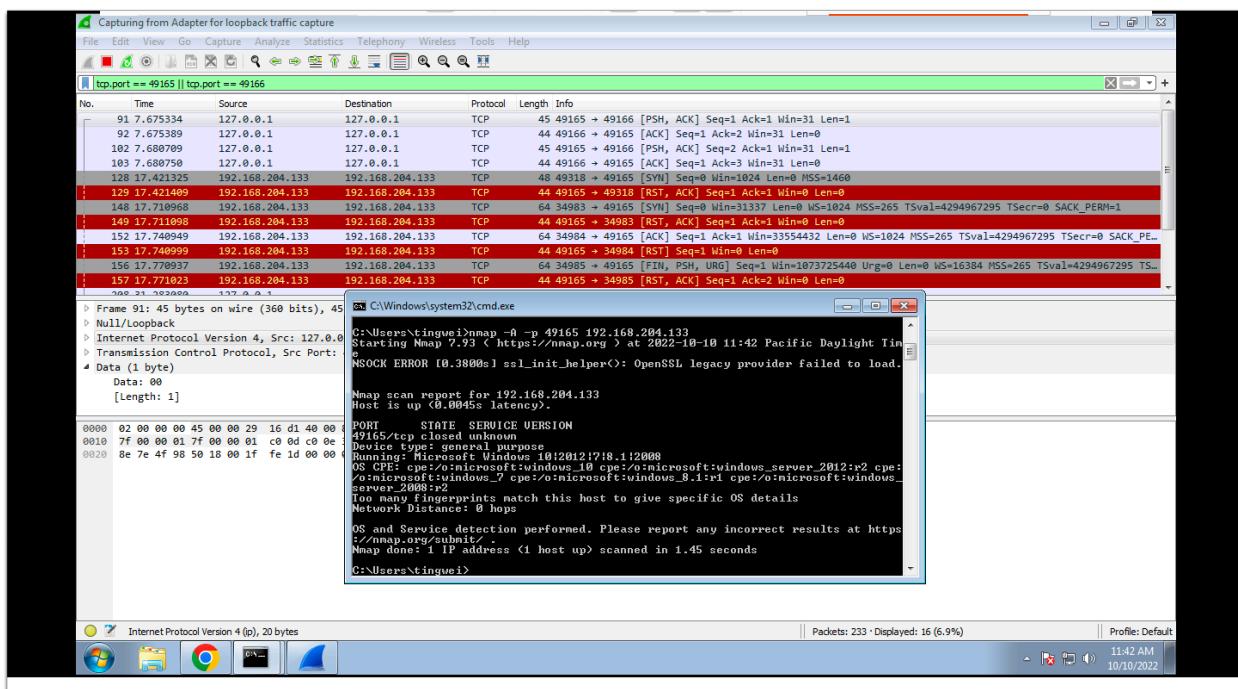


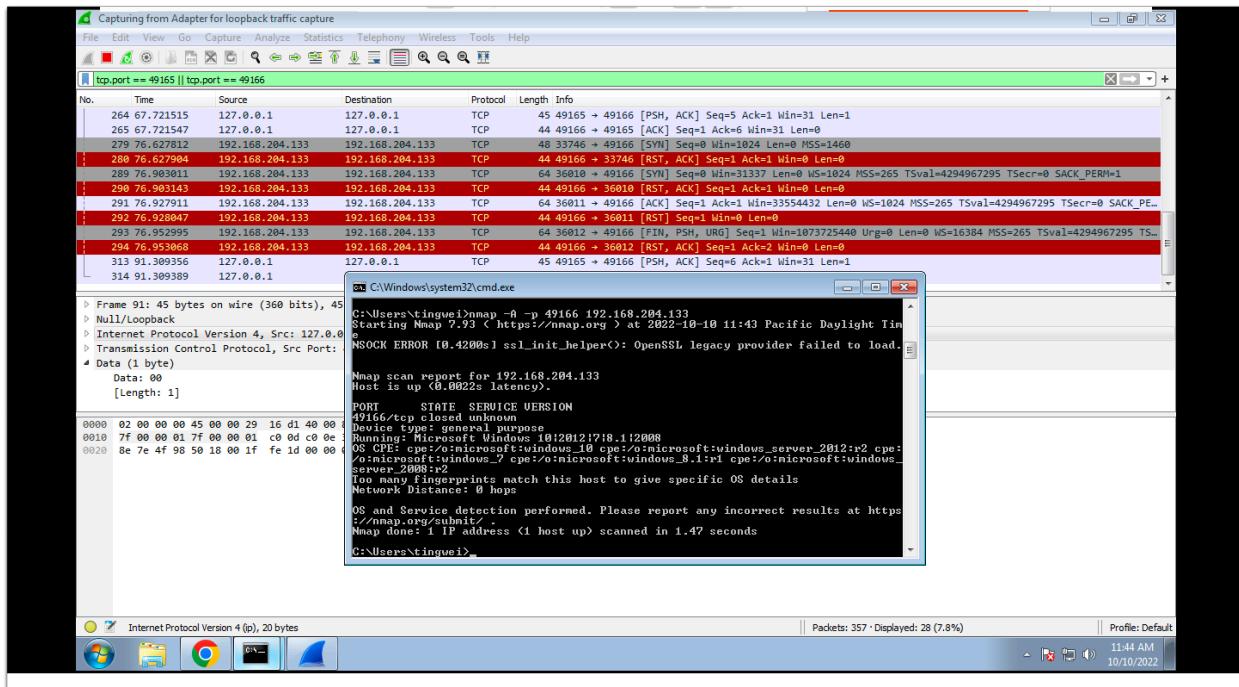
The data sending frequency is unstable. From my observation, the frequency gets higher when I interacts with the web interface of ScadaBR. If I did not interact with ScadaBR, then there's no traffic.



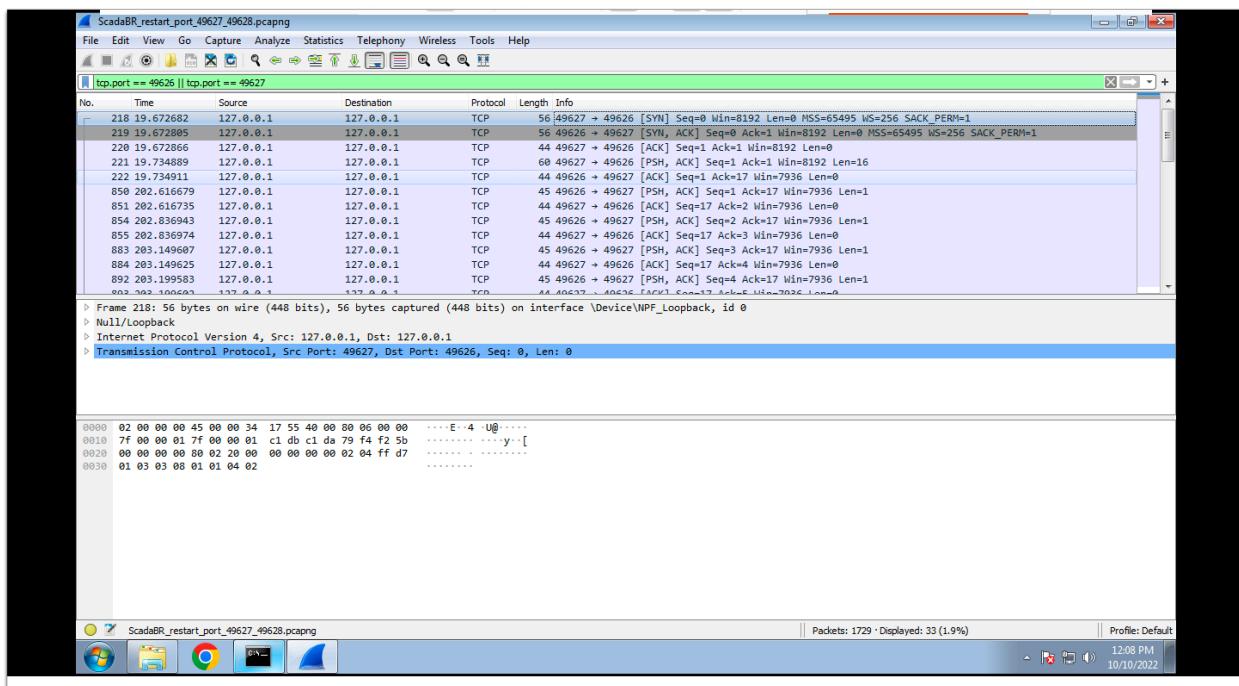
Here's the result

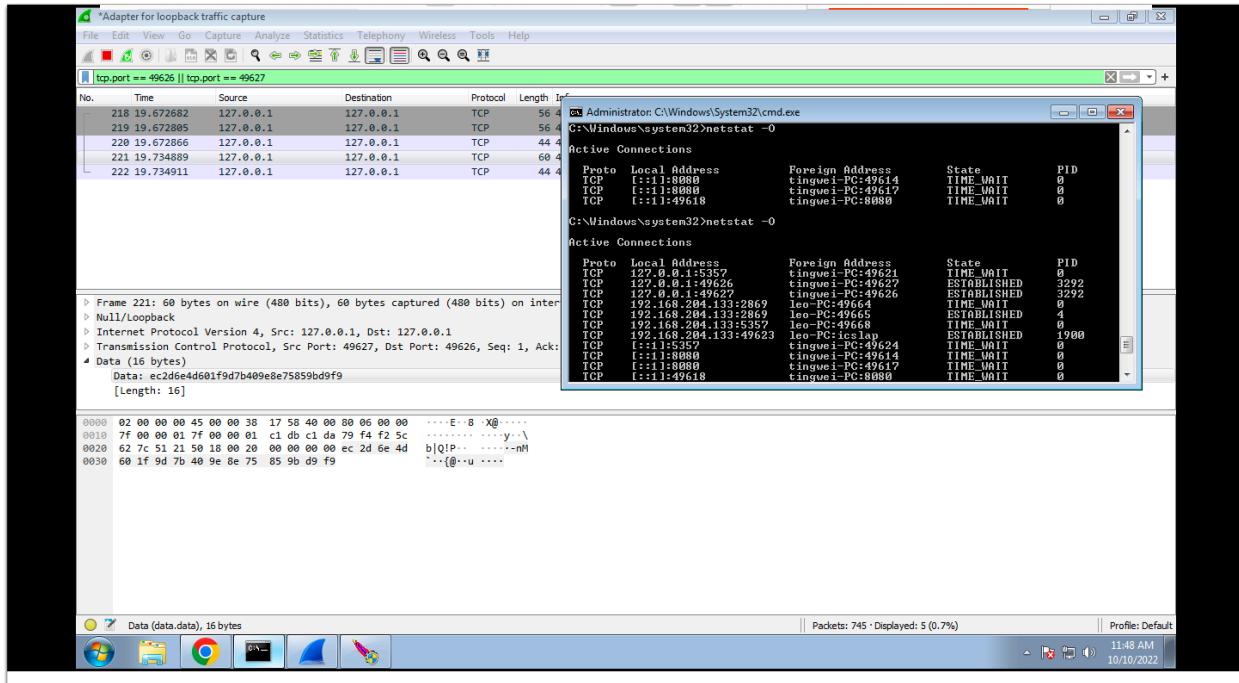
from Nmap. It disconnects immediately when I tried to connect to it. And it does not provide any information about the service.



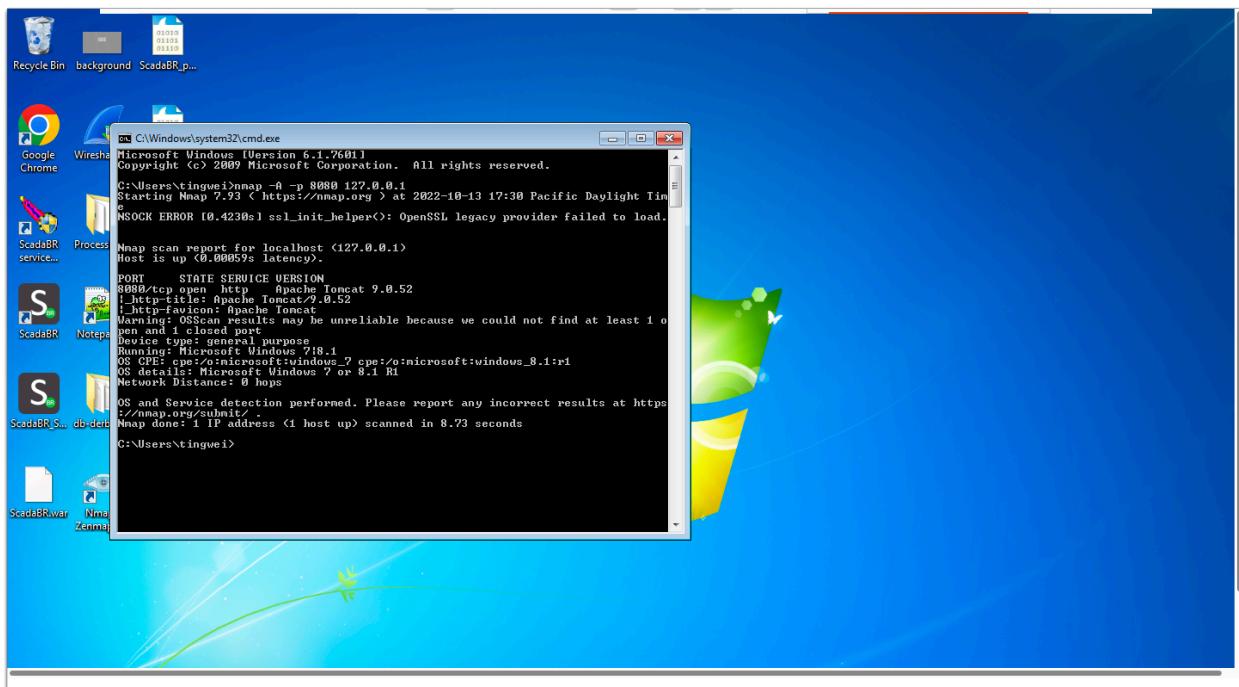


I restart ScadaBR service to do some observation on its connections. The traffic is in "ScadaBR_restart_port_49627_49628.pcapng". It shows that it sends a 16 bytes encrypted data at the beginning. But after that, every thing is 0.

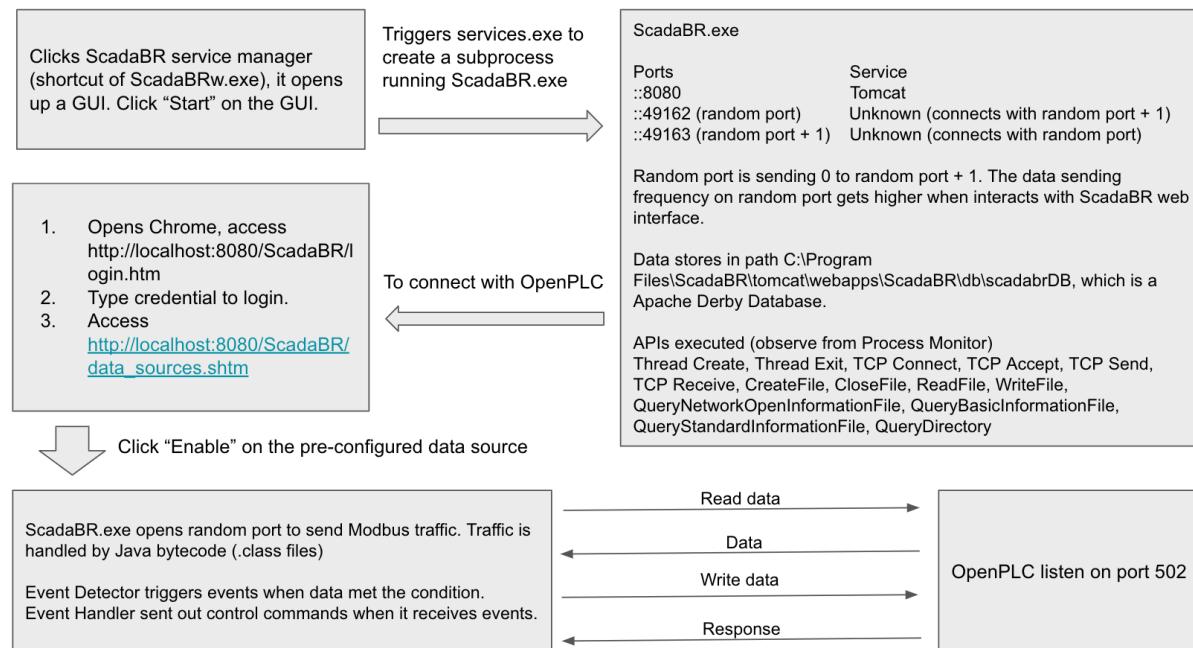




On the other hand, as expected, port 8080 is hosting Apache Tomcat.



ScadaBR Interactions



Additional Information about Database

There is a database interaction panel on ScadaBR web interface. We can search data in the database from there.

Data Source

The screenshot shows the ScadaBR 1.2 web interface with the URL localhost:8080/ScadaBR/sql.shtm. The page has a green header bar with the ScadaBR logo and navigation icons. Below the header is a warning message: "Warning: use this facility at your own risk. Incorrect usage may result in corrupted data and/or system failures." A SQL input field contains the query "SELECT * FROM dataSources". Below the input field are two buttons: "Submit query" and "Submit update". A table below the input field displays the results of the query:

ID	XID	NAME	DATASOURCETYPE	DATA
1	DS_132410	OpenPLC_Windows_3	Serialized data	com.serotonin.mango.vo.dataSource.modbus.ModbusDataSourceVO@5f1ee933)

At the bottom of the page, there is a copyright notice: "©2009-present Fundação Certi, MCA Sistemas, Unis Sistemas, Conetec. All rights reserved." The status bar at the bottom right shows the time as 12:59 PM and the date as 10/12/2022.

Data Points

Warning: use this facility at your own risk. Incorrect usage may result in corrupted data and/or system failures.

SQL `SELECT * FROM datapoints`

ID	XID	DATA SOURCE ID	DATA
1	DP_164875	1	Serialized data(DataPointVO {id=0, xid=null, name=RedLight, dataSourceId=0, deviceName=OpenPLC_Windows, enabled=true, pointFolderId=0, loggingType=1, intervalLoggingPeriodType=2, intervalLoggingPeriod=15, intervalLoggingType=1, tolerance=0.0, purgeType=7, purgePeriod=1, textRenderer=com.serotonin.mango.view.text.PlainRenderer@355aa9a1, chartRenderer=null, eventDetectors=null, comments=null, defaultCacheSize=1, discardExtremeValues=false, discardLowLimit=-1.797693134623157E308, discardHighLimit=1.797693134623157E308, engineeringUnits=95, chartColour=null, pointLocator=com.serotonin.mango.vo.dataSource.modbus.ModbusPointLocatorVO@447e5f6, dataSourceTypeId=0, dataSourceName=null, dataSourceXid=null, lastValue=null, settable=false})
2	DP_807241	1	Serialized data(DataPointVO {id=0, xid=null, name=OrangeLight, dataSourceId=0, deviceName=OpenPLC_Windows, enabled=true, pointFolderId=0, loggingType=1, intervalLoggingPeriodType=2, intervalLoggingPeriod=15, intervalLoggingType=1, tolerance=0.0, purgeType=7, purgePeriod=1, textRenderer=com.serotonin.mango.view.text.PlainRenderer@14db3c2d, chartRenderer=null, eventDetectors=null, comments=null, defaultCacheSize=1, discardExtremeValues=false, discardLowLimit=-1.797693134623157E308, discardHighLimit=1.797693134623157E308, engineeringUnits=95, chartColour=null, pointLocator=com.serotonin.mango.vo.dataSource.modbus.ModbusPointLocatorVO@42e88b6, dataSourceTypeId=0, dataSourceName=null, dataSourceXid=null, lastValue=null, settable=false})
3	DP_882433	1	Serialized data(DataPointVO {id=0, xid=null, name=GreenLight, dataSourceId=0, deviceName=OpenPLC_Windows, enabled=true, pointFolderId=0, loggingType=1, intervalLoggingPeriodType=2, intervalLoggingPeriod=15, intervalLoggingType=1, tolerance=0.0, purgeType=7, purgePeriod=1, textRenderer=com.serotonin.mango.view.text.PlainRenderer@4a0e58a6, chartRenderer=null, eventDetectors=null, comments=null, defaultCacheSize=1, discardExtremeValues=false, discardLowLimit=-1.797693134623157E308, discardHighLimit=1.797693134623157E308, engineeringUnits=95, chartColour=null, pointLocator=com.serotonin.mango.vo.dataSource.modbus.ModbusPointLocatorVO@49e180, dataSourceTypeId=0, dataSourceName=null, dataSourceXid=null, lastValue=null, settable=false})
4	DP_996277	1	Serialized data(DataPointVO {id=0, xid=null, name=HMI_EmergencyGreenPb, dataSourceId=0, deviceName=OpenPLC_Windows, enabled=true, pointFolderId=0, loggingType=1, intervalLoggingPeriodType=2, intervalLoggingPeriod=15, intervalLoggingType=1, tolerance=0.0, purgeType=7, purgePeriod=1, textRenderer=com.serotonin.mango.view.text.PlainRenderer@5410d416, chartRenderer=null, eventDetectors=null, comments=null, defaultCacheSize=1, discardExtremeValues=false, discardLowLimit=-1.797693134623157E308, discardHighLimit=1.797693134623157E308, engineeringUnits=95, chartColour=null, pointLocator=com.serotonin.mango.vo.dataSource.modbus.ModbusPointLocatorVO@62533dc, dataSourceTypeId=0, dataSourceName=null, dataSourceXid=null, lastValue=null, settable=false})
5	DP_740260	1	Serialized data(DataPointVO {id=0, xid=null, name=PI_Fedelito, dataSourceId=0, deviceName=OpenPLC_Windows, enabled=true, pointFolderId=0, loggingType=1, intervalLoggingPeriodType=2, intervalLoggingPeriod=15, intervalLoggingType=1, tolerance=0.0, purgeType=7, purgePeriod=1, textRenderer=com.serotonin.mango.view.text.PlainRenderer@300d21d3, chartRenderer=null, eventDetectors=null, comments=null, defaultCacheSize=1, discardExtremeValues=false, discardLowLimit=-1.797693134623157E308, discardHighLimit=1.797693134623157E308, engineeringUnits=95, chartColour=null, pointLocator=com.serotonin.mango.vo.dataSource.modbus.ModbusPointLocatorVO@626ff3a0, dataSourceTypeId=0, dataSourceName=null, dataSourceXid=null, lastValue=null, settable=false})

Event Detector

Warning: use this facility at your own risk. Incorrect usage may result in corrupted data and/or system failures.

SQL `SELECT * FROM pointEventDetectors`

ID	XID	ALIAS	DATAPOINTID	DETECTORTYPE	ALARMLEVEL	STATELIMIT	DURATION	DURATIONTYPE	BINARYSTATE	MULTISTATESTATE	CHANGECOUNT	ALPHANUMERICSTAT
2	PED_177817		1	6	0	0.0	10	1	N	0	2	

Event Handler

ScadaBR 1.2 +

localhost:8080/ScadaBR/sql.htm

scadaBR Urgent

Warning: use this facility at your own risk. Incorrect usage may result in corrupted data and/or system failures.

SQL SELECT * FROM eventHandlers

Submit query | Submit update

ID	XID	ALIAS	EVENTTYPEID	EVENTTYPEREF1	EVENTTYPEREF2	DATA
3	activate_emergency	activate_emergency	1	2		Serialized data(com.serotonin.mango.vo.event.EventHandlerVO@26449545)

©2009-present Fundação Certi, MCA Sistemas, Unis Sistemas, Conetec. All rights reserved.

1:04 PM
10/12/2022

The screenshot shows a web browser window titled 'ScadaBR 1.2' with the URL 'localhost:8080/ScadaBR/sql.htm'. The page has a green header bar with the 'scadaBR' logo and an 'Urgent' button. A warning message at the top states: 'Warning: use this facility at your own risk. Incorrect usage may result in corrupted data and/or system failures.' Below this is a SQL input field containing the query 'SELECT * FROM eventHandlers'. Two buttons, 'Submit query' and 'Submit update', are located below the input field. The main content area displays a table with the following data:

ID	XID	ALIAS	EVENTTYPEID	EVENTTYPEREF1	EVENTTYPEREF2	DATA
3	activate_emergency	activate_emergency	1	2		Serialized data(com.serotonin.mango.vo.event.EventHandlerVO@26449545)

At the bottom of the page, there is a copyright notice: '©2009-present Fundação Certi, MCA Sistemas, Unis Sistemas, Conetec. All rights reserved.'