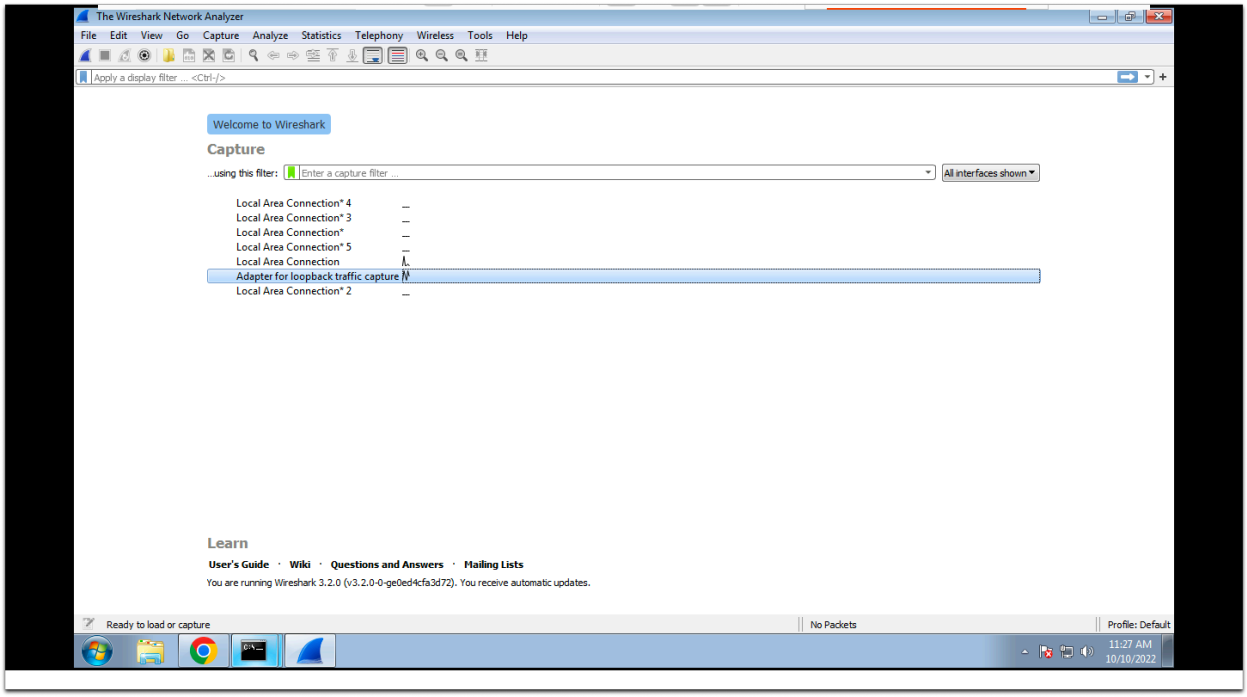
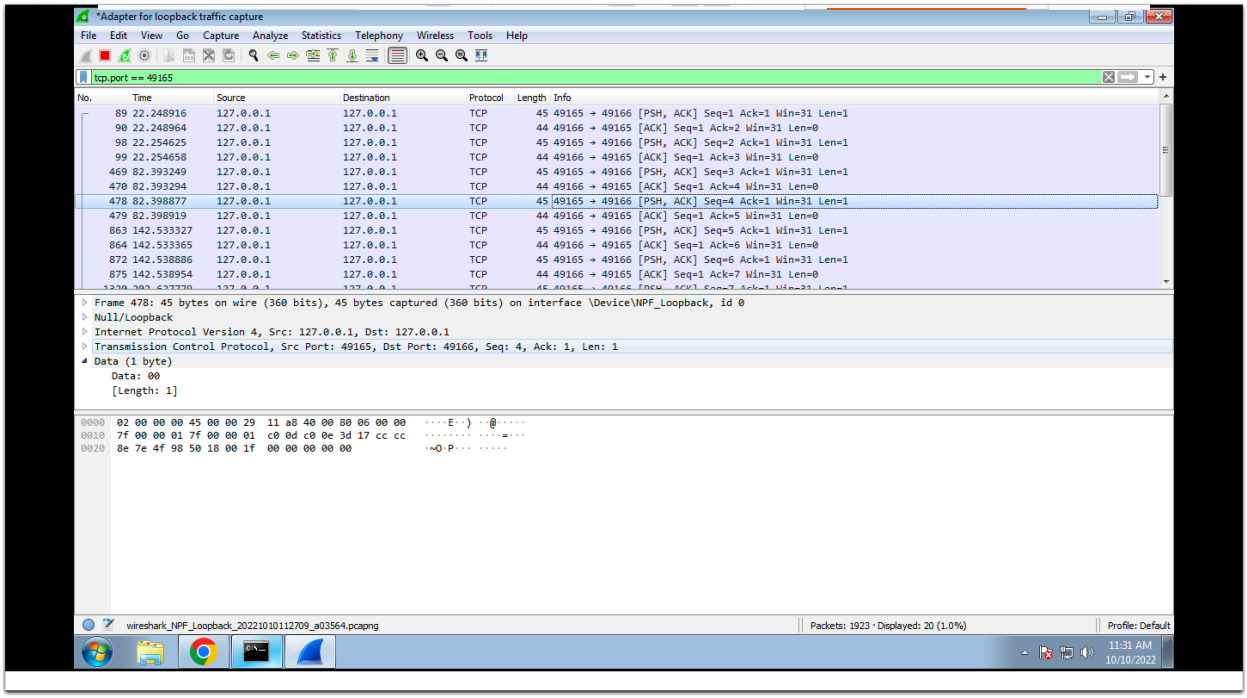
Observation on ports by ScadaBR.exe

I did research with both Wireshark and Nmap.

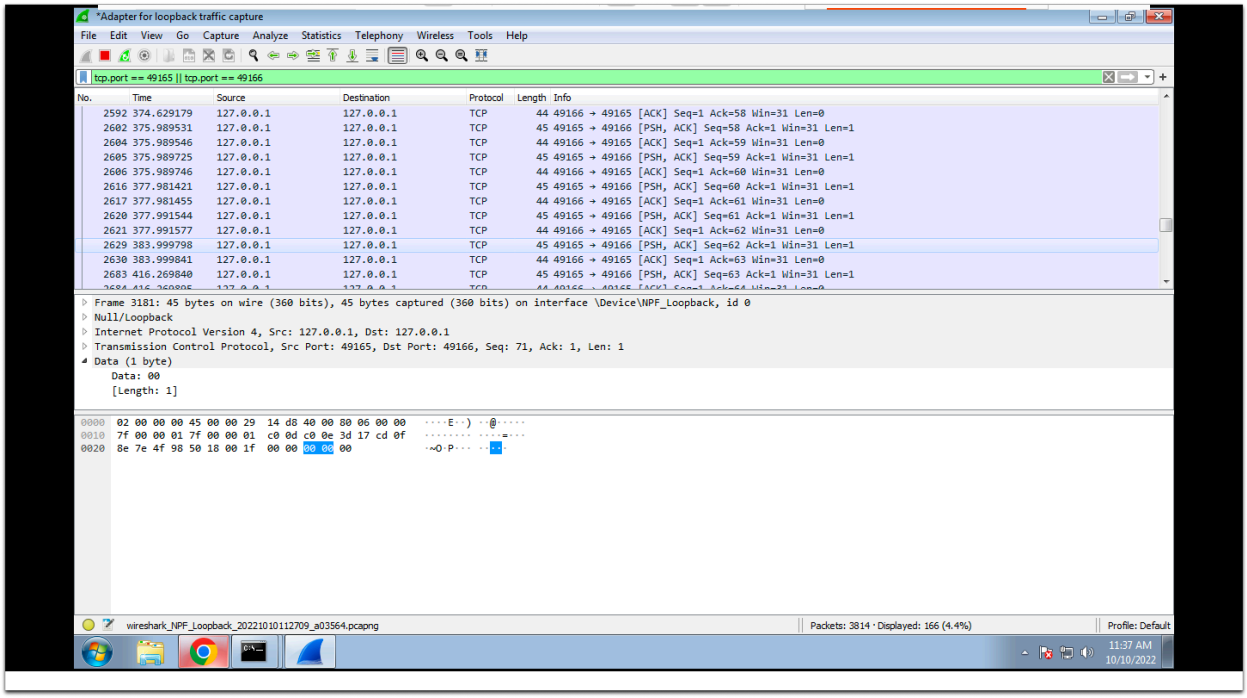
Select the loopback interface to fetch traffic sending to host itself.
The traffic is saved as attachment “ScadaBR_port_49165_49166_traffic.pcapng”



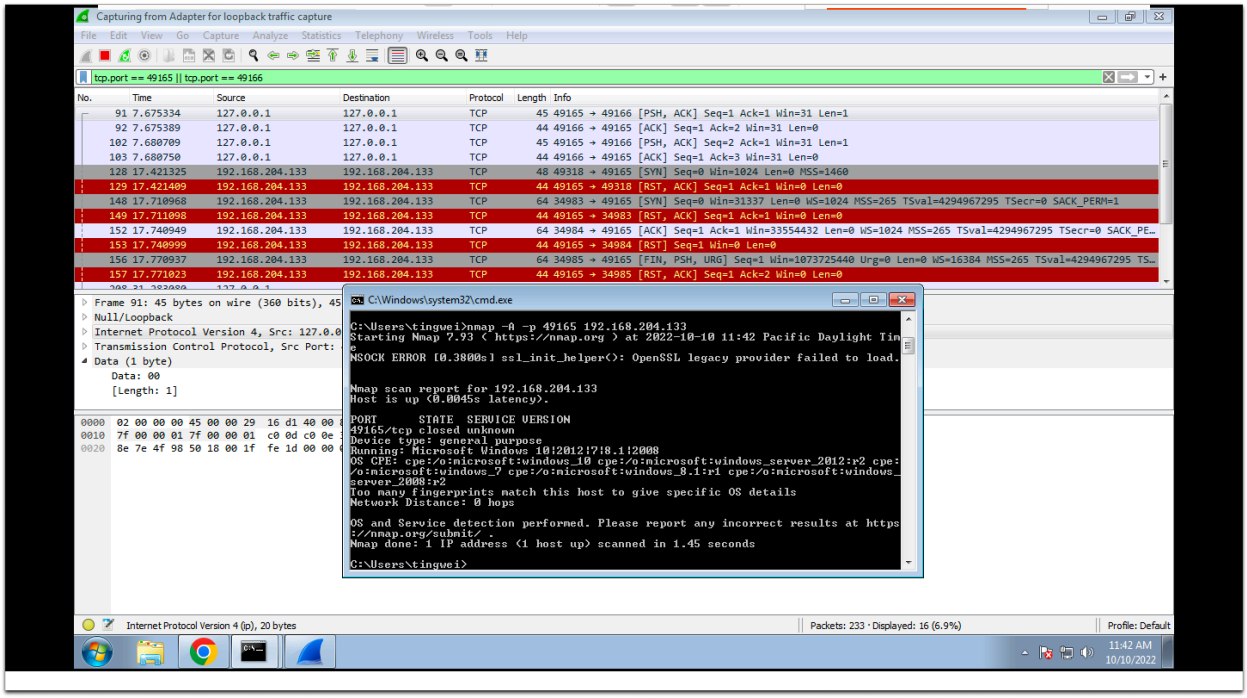
From the observation, I found that the lower value port is always sending Data 0 to the higher port, even if I did some interaction with ScadaBR web interface.

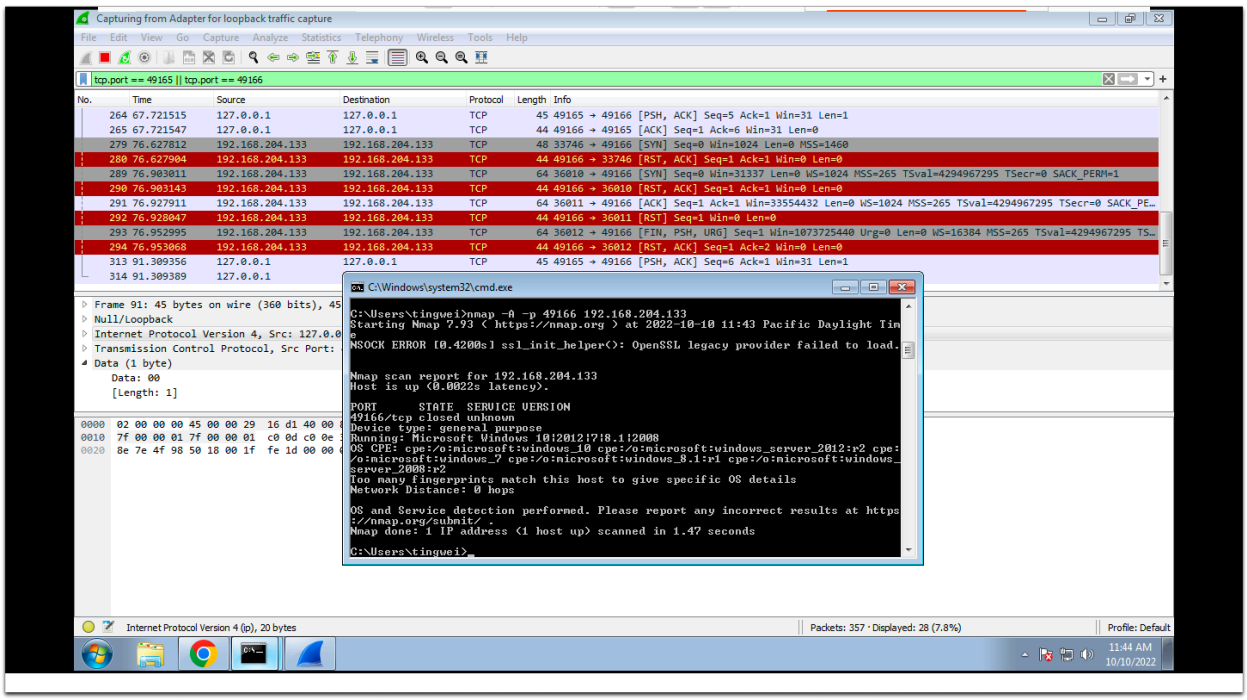


The data sending frequency is unstable. From my observation, the frequency gets higher when I interacts with the web interface of ScadaBR. If I did not interact with ScadaBR, then there's no traffic.

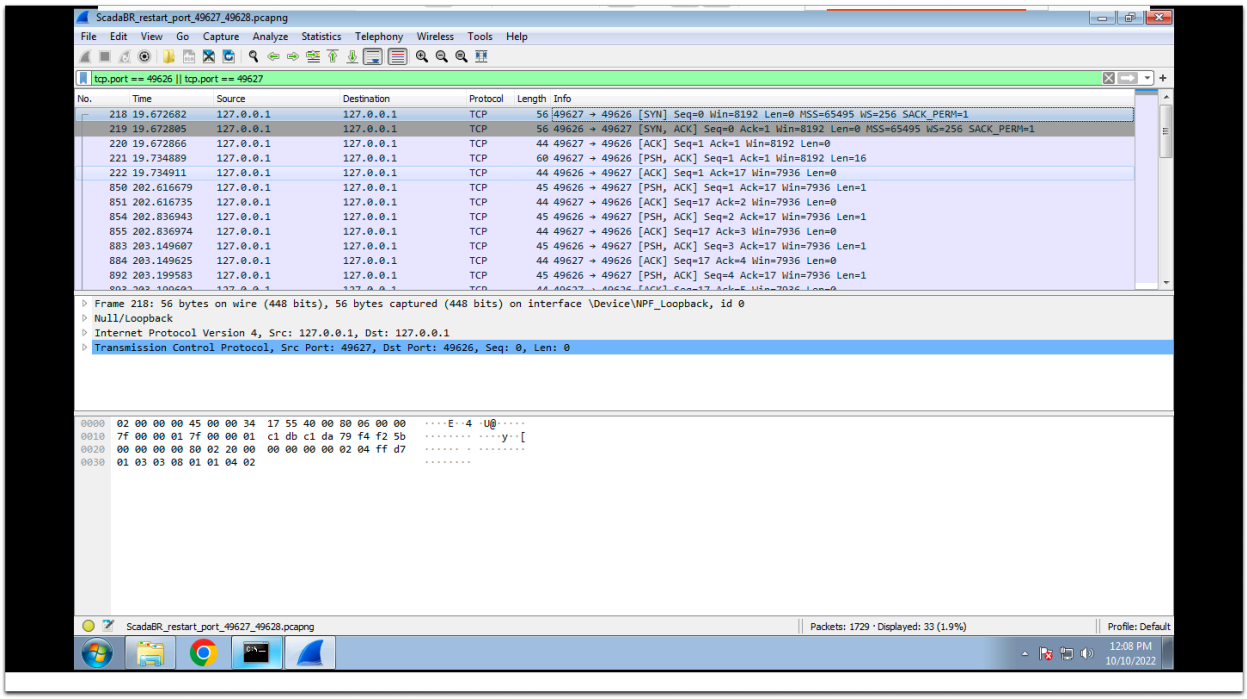


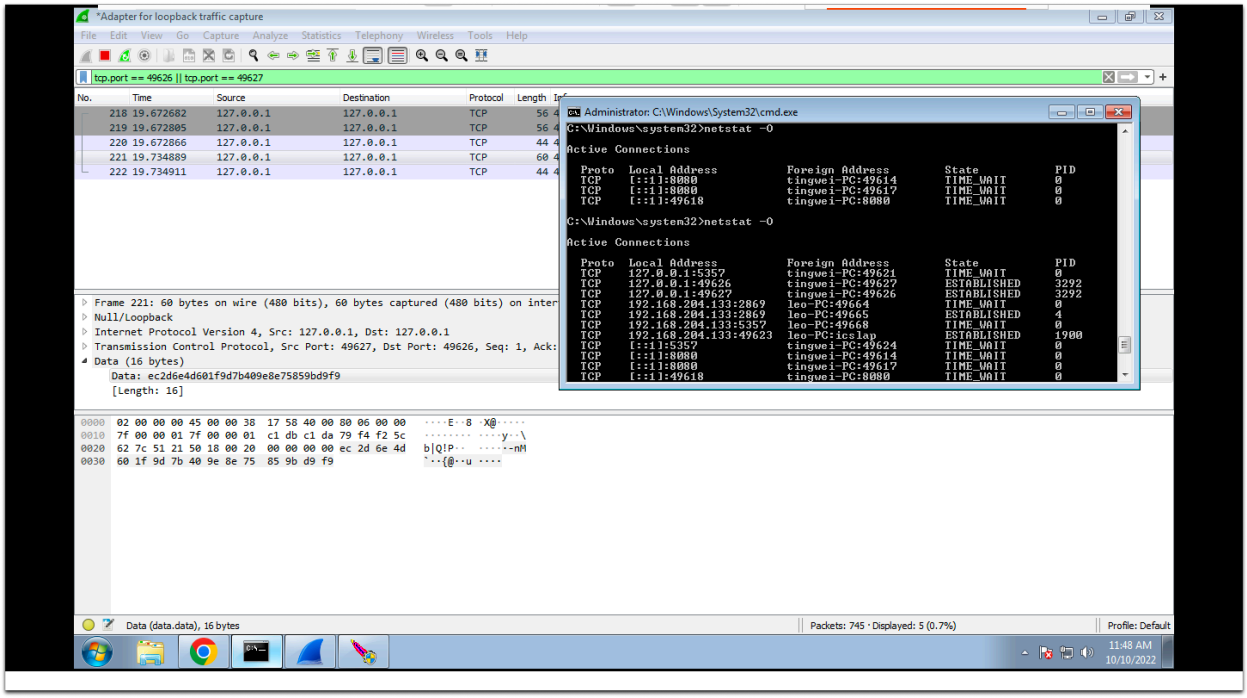
Here's the result
from Nmap. It disconnects immediately when I tried to connect to it. And it does not provide any information about the service.



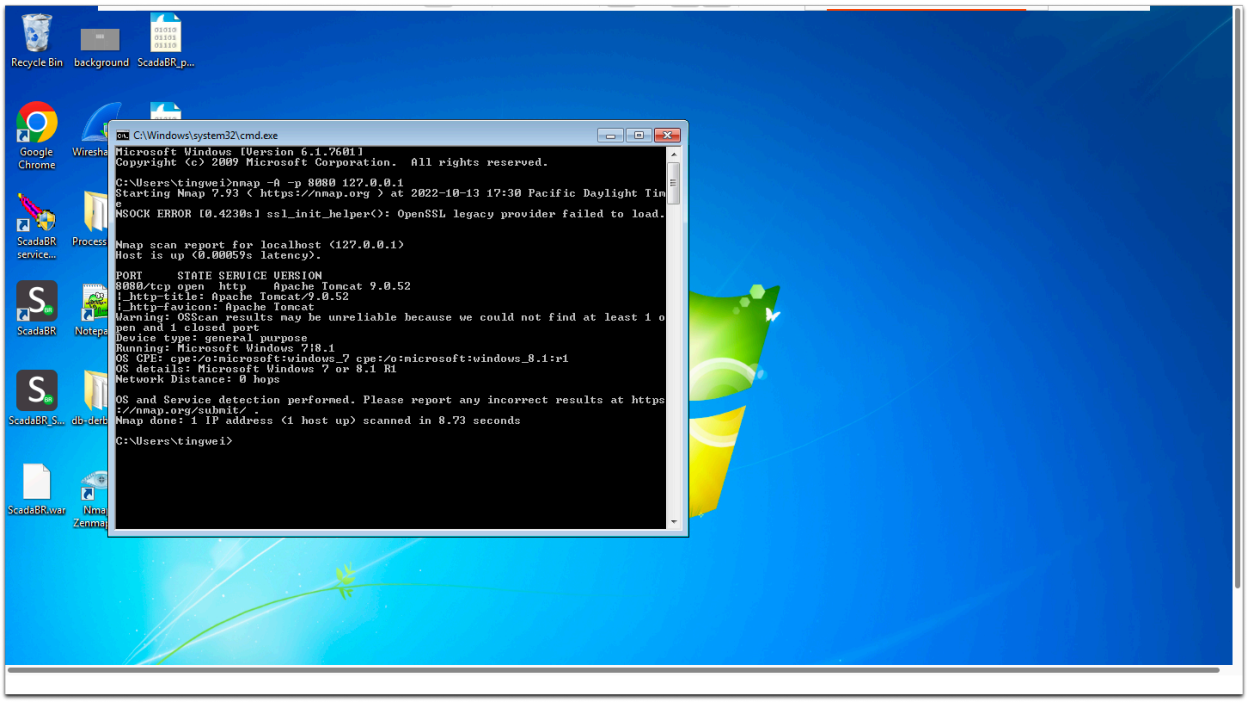


I restart ScadaBR service to do some observation on its connections. The traffic is in “ScadaBR_restart_port_49627_49628.pcapng”
It shows that it sends a 16 bytes encrypted data at the beginning. But after that, every thing is 0.

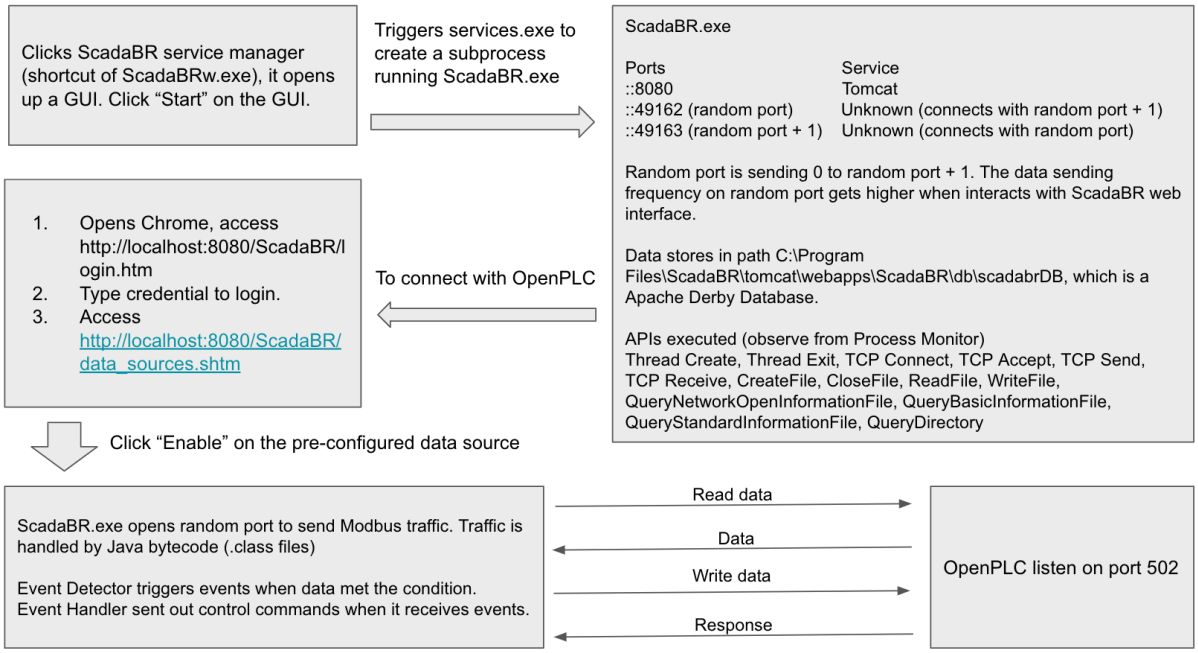




On the other hand, as expected, port 8080 is hosting Apache Tomcat.



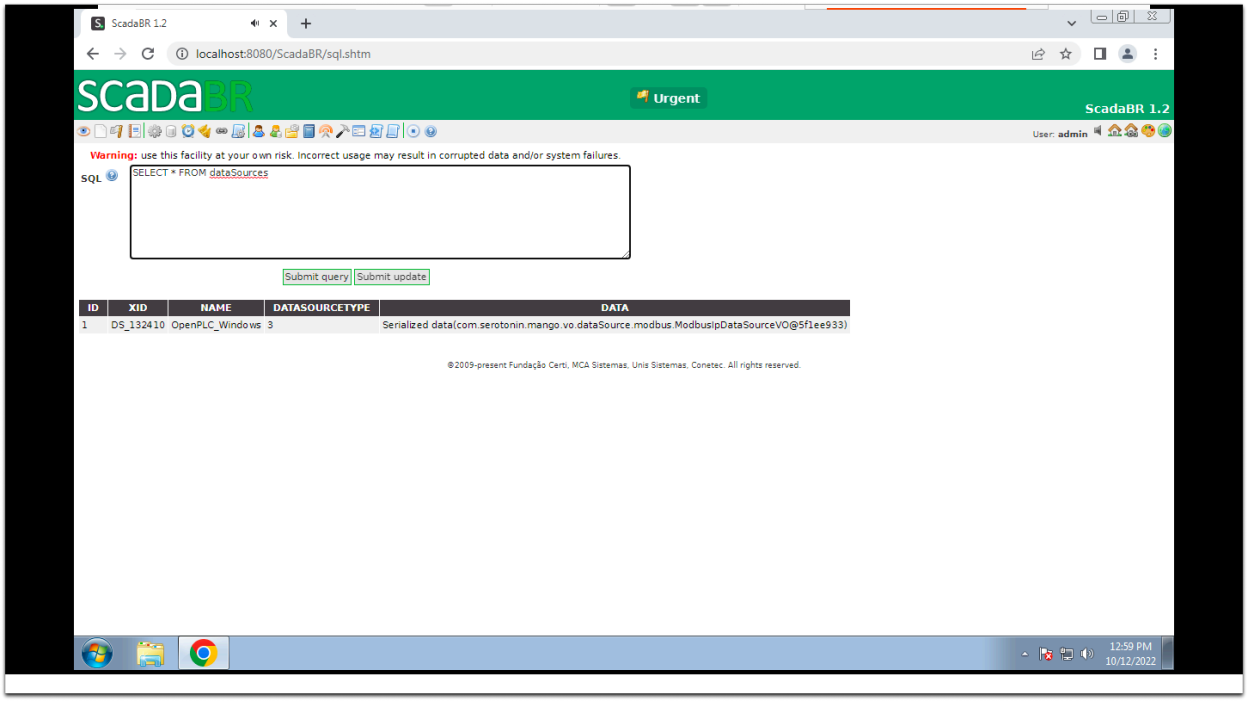
ScadaBR Interactions



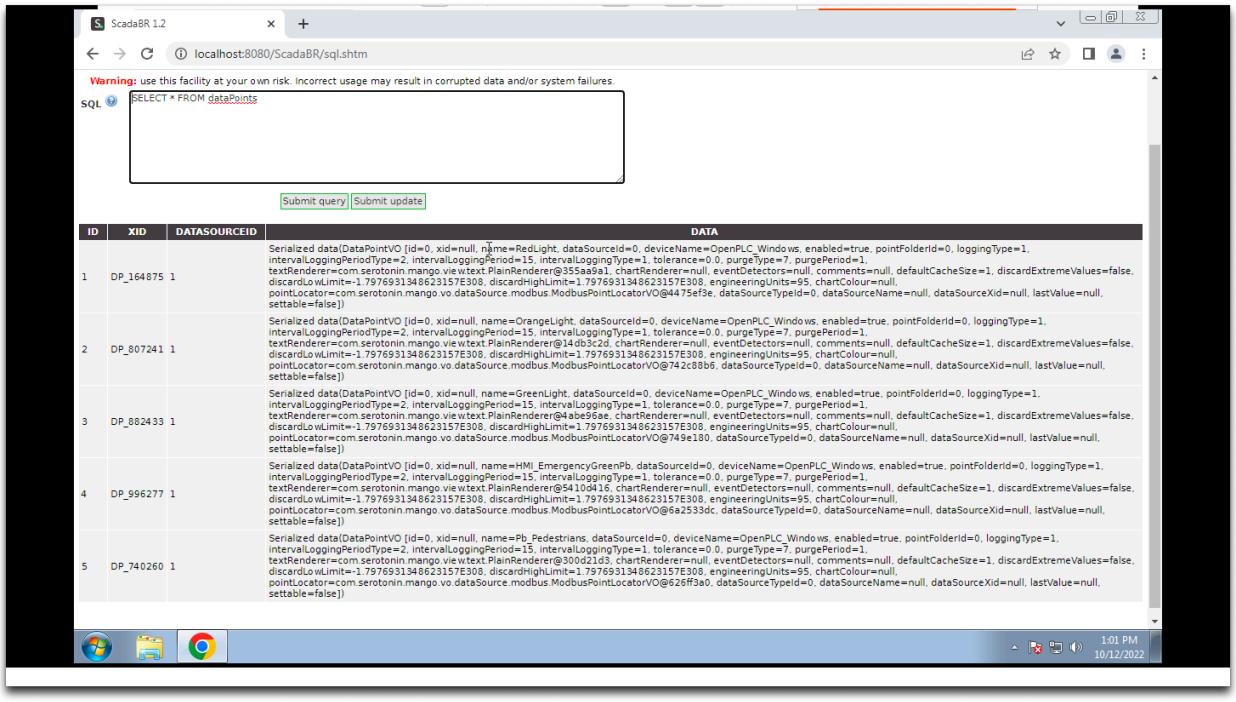
Additional Information about Database

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

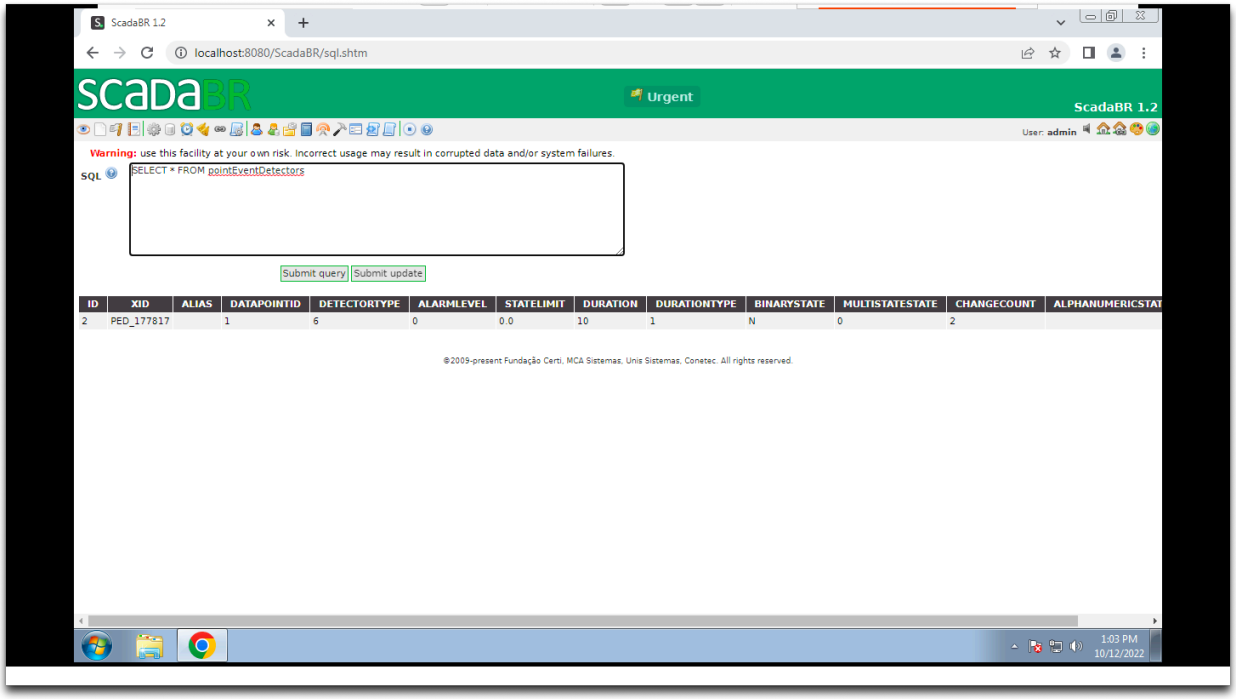
Data Source



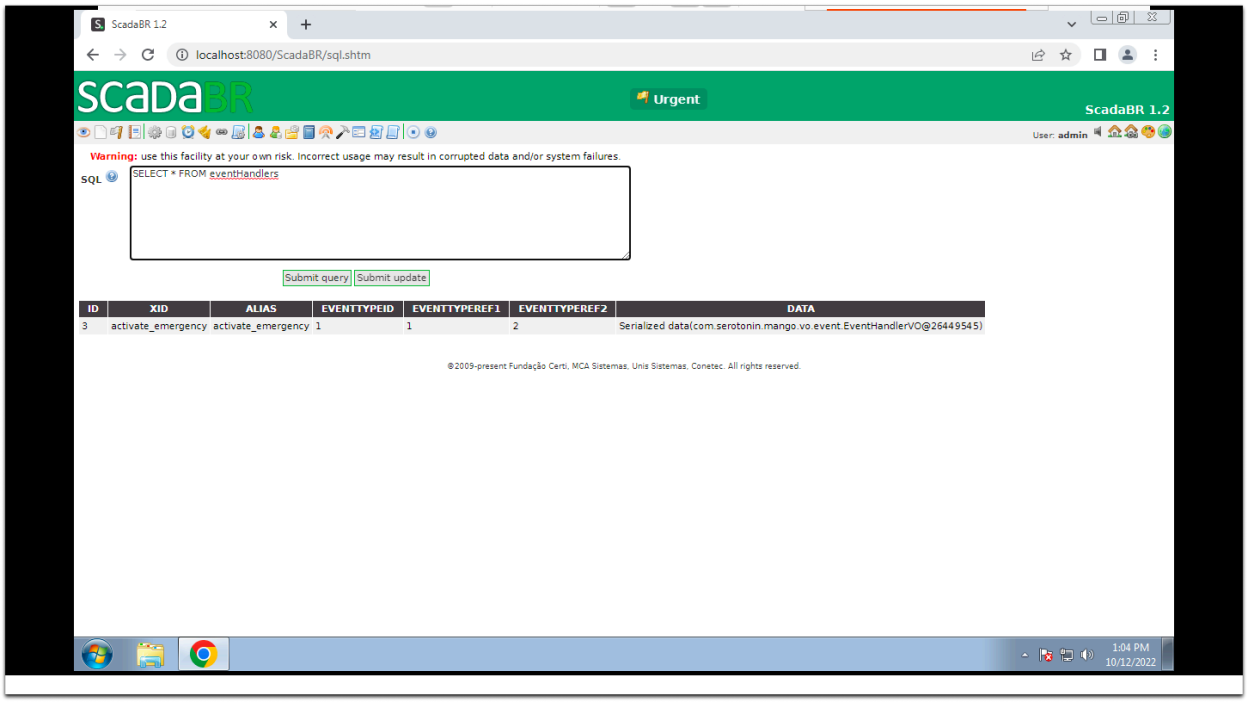
Data Points



Event Detector



Event Handler


ScadaBR 1.2
localhost:8080/ScadaBR/sql.shtm
scadaBR
Urgent
ScadaBR 1.2
User: admin
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
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