How to Capture, Parse and Troubleshoot SNMP traps using Wireshark

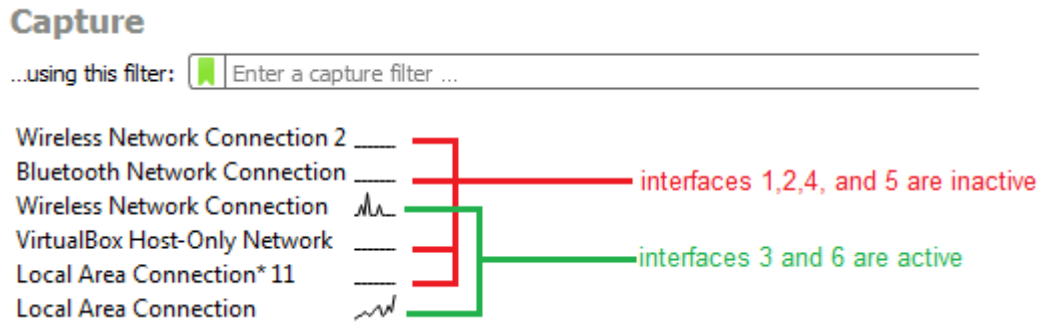
https://campus.barracuda.com/doc/93200916/

This article describes how to verify the Barracuda RMM is parsing traps properly as they are received by the system it is installed on. Unlike iReasoning's trap receiver, it is not necessary to stop the MWExpertSystem while troubleshooting when using Wireshark, which is useful when solving long-term or intermittent issues.

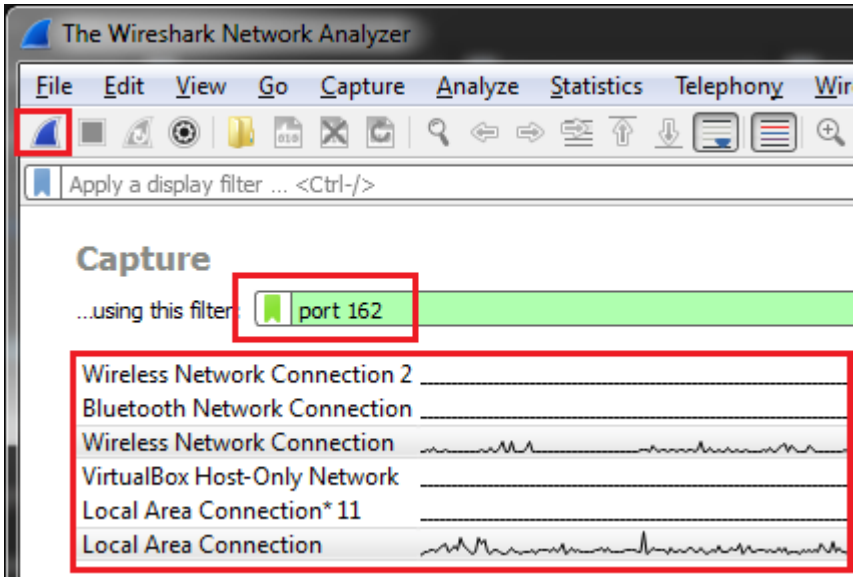
Since the wincap driver grabs packets as soon as they hit a port, before a software firewall can block them, Wireshark can monitor traffic on port 162 while MWExpertSystem is running.

To enable Wireshark monitoring

1. Install Wireshark - including the installer's WinPcap driver.
2. Start Wireshark and take note of which interface(s) are active (sending and receiving traffic):



3. Do one of the following:
   - If you are going to be capturing for a short period of time, for example, while you are on the phone, enter the following capture filter: port 162 and select the two interfaces. Click the blue shark fin on the top right to start capturing.

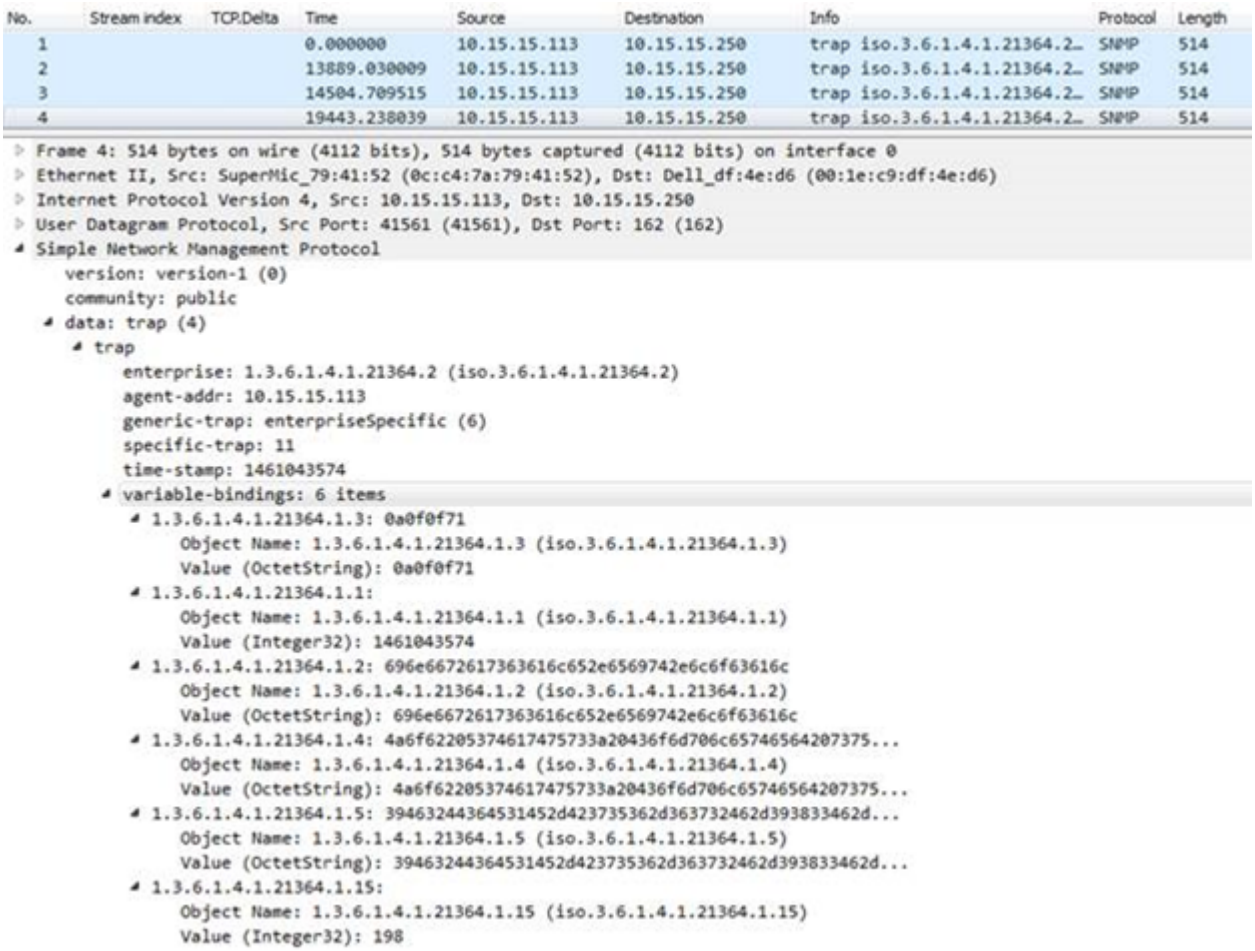


- If you want a long term capture, start up the capture using tshark.exe from the command line instead, making sure to specify an output file and stop condition. Information about the command line options is available here. An example of this would be:

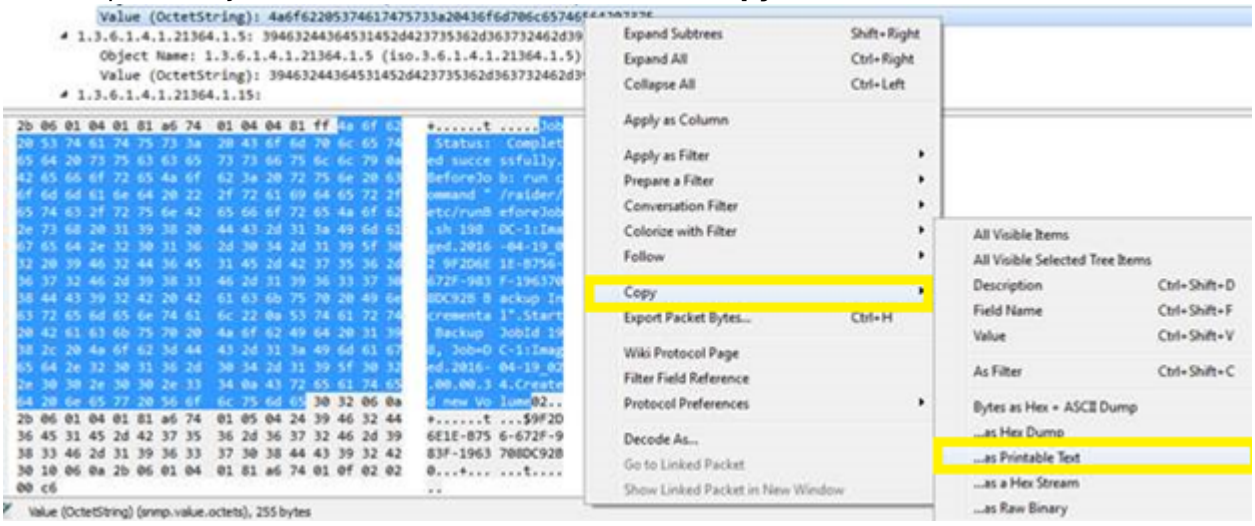
```
"c:\Program Files\Wireshark\tshark.exe" -i 3 -i 6 -f "port 162" -a filesize:10240 -w "C:\Temp\snmptraptrace.pcapng"
```

  where the -i flags indicate which interface to capture, -a indicated the stop condition 10mb of capture) and -w is the output file. You can use `-a duration:600 ` instead to stop after 10 minutes (duration is in seconds).

4. Once you've captured the data, you will see the list of received UDP packets. Selecting a packet will give you additional information if you expand the **Simple Network Management Protocol** tree. This information includes the SNMP version, the community string, the enterprise OIDs, and variable bindings:



5. You will notice that most values are either Integers or OctetStrings. The string values are displayed in hexadecimal by default, but you can see a pageview of the string values in the bottom pane, or you can rick clock on the value and **Copy** > **as Printable Text**.



6. This lets you paste the textual value which you can use to help create or verify monitoring rules. For example:

"Job Status: Completed successfully
BeforeJob: run command "/raider/etc/runBeforeJob.sh 198 DC-1:Imaged.2016-04-19_02 9F2D6E1E-B756-672F-983F-1963708DC92B Backup Incremental"
Start Backup JobId 198, Job=DC-1:Imaged.2016-04-19_02.00.00.34
Created new Volume"

Figures

1. clipboard_e0241695bacdbb4a3a427d0bb413810dc.png
2. clipboard_e4fb84e733770b631960895b62bf0b38c.png
3. clipboard_e335f48ce0b1c1528e2728d99394d1434.png
4. clipboard_e74d6061db0fb68b34e095c3237941fa6.png
5. clipboard_e3872d9c5986621f139e0df006a65705a.png
6. clipboard_ea04ad2f817bb85831aa1314618380881.png