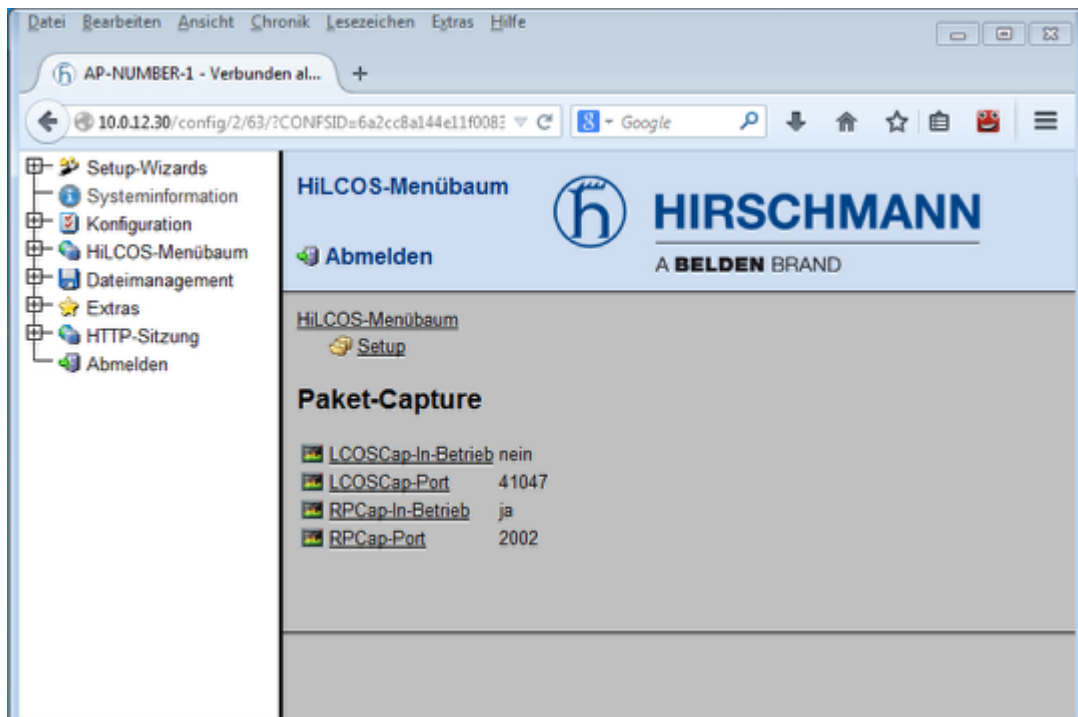


## How to remotely capture the traffic of an Open BAT interface with RPCap function and Wireshark

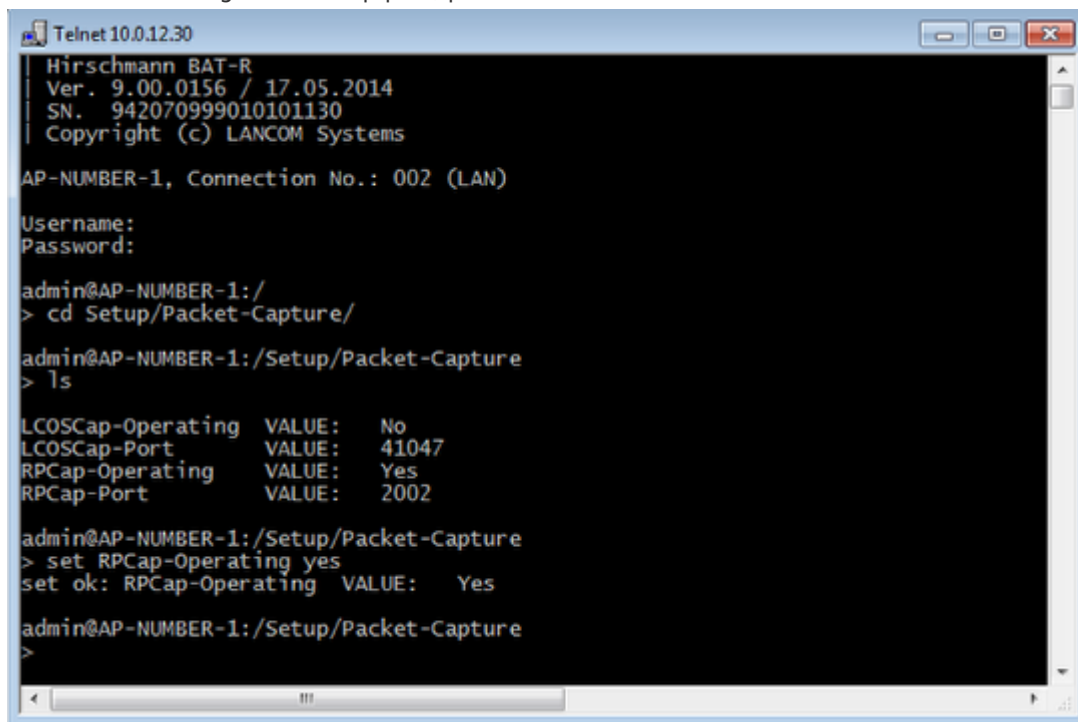
- 2018-02-21 - BAT, WLC (HiLCOS)

This lesson explains via a few steps how to use the RPCap function to capture traffic remotely on specific interface(s) of the BAT devices (rel 8.90)

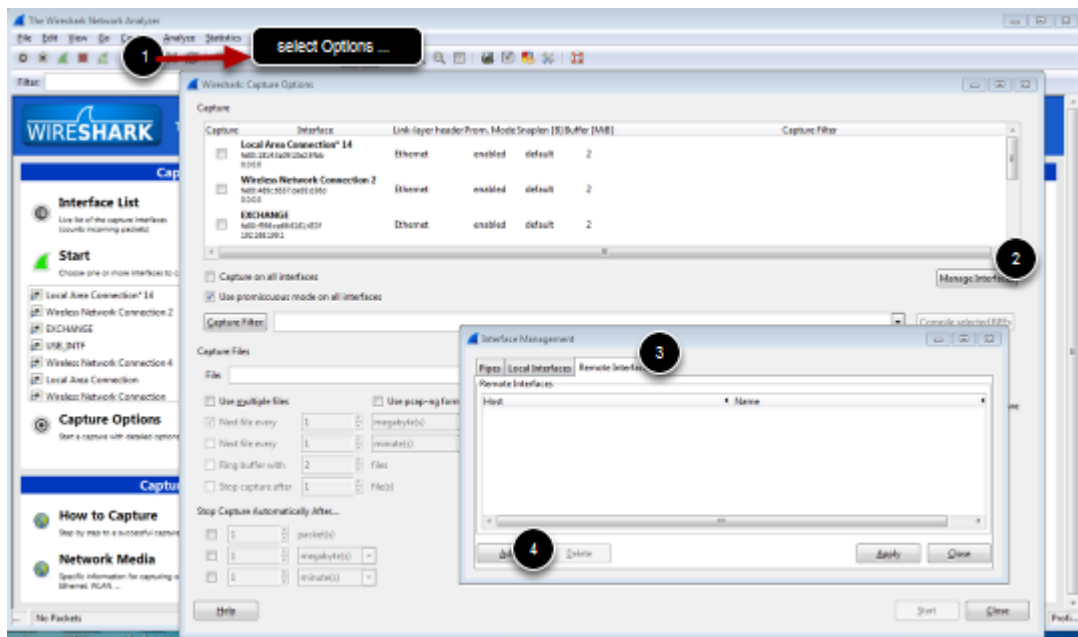
**Enable RPCap on the BAT using the web interface or per CLI**



You can also change the RPCap port, per default it's 2002

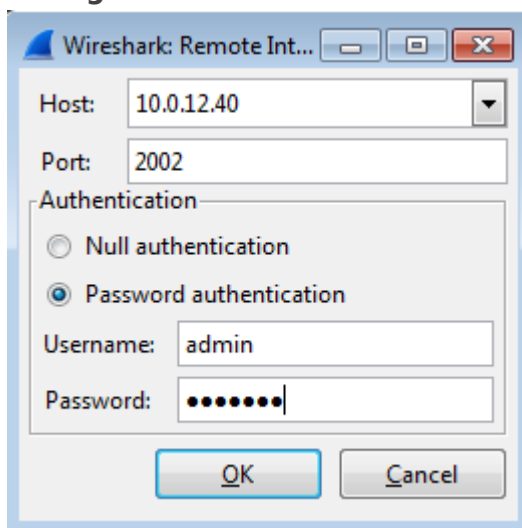


Add remote interfaces in wireshark options



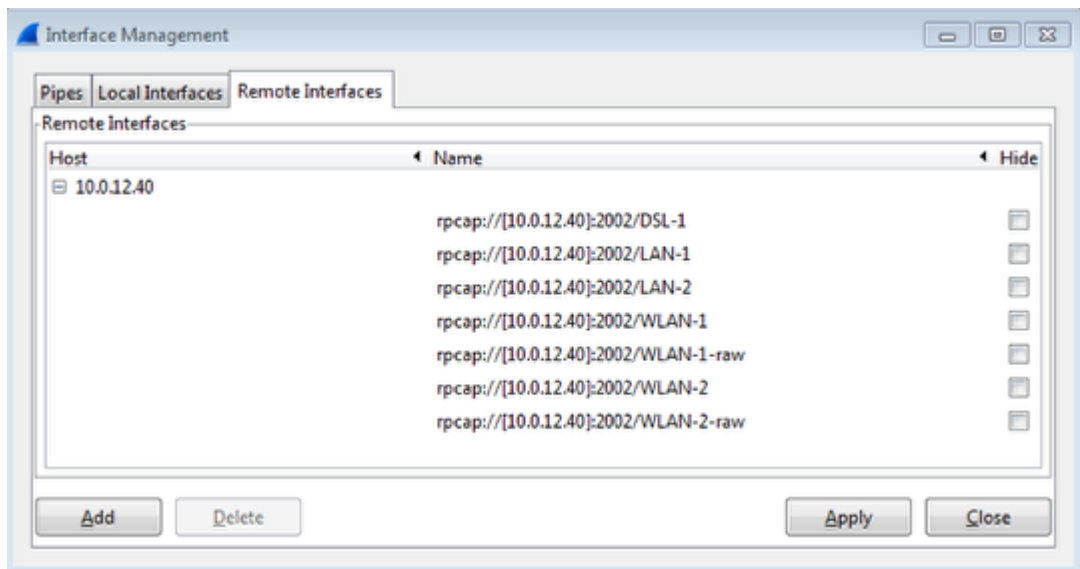
From Wireshark main Windows, open the Capture Options window (Capture/Options...). Click on manage Interface and select the tab Remote Interfaces and click on Add

### Configure the BAT as remote device



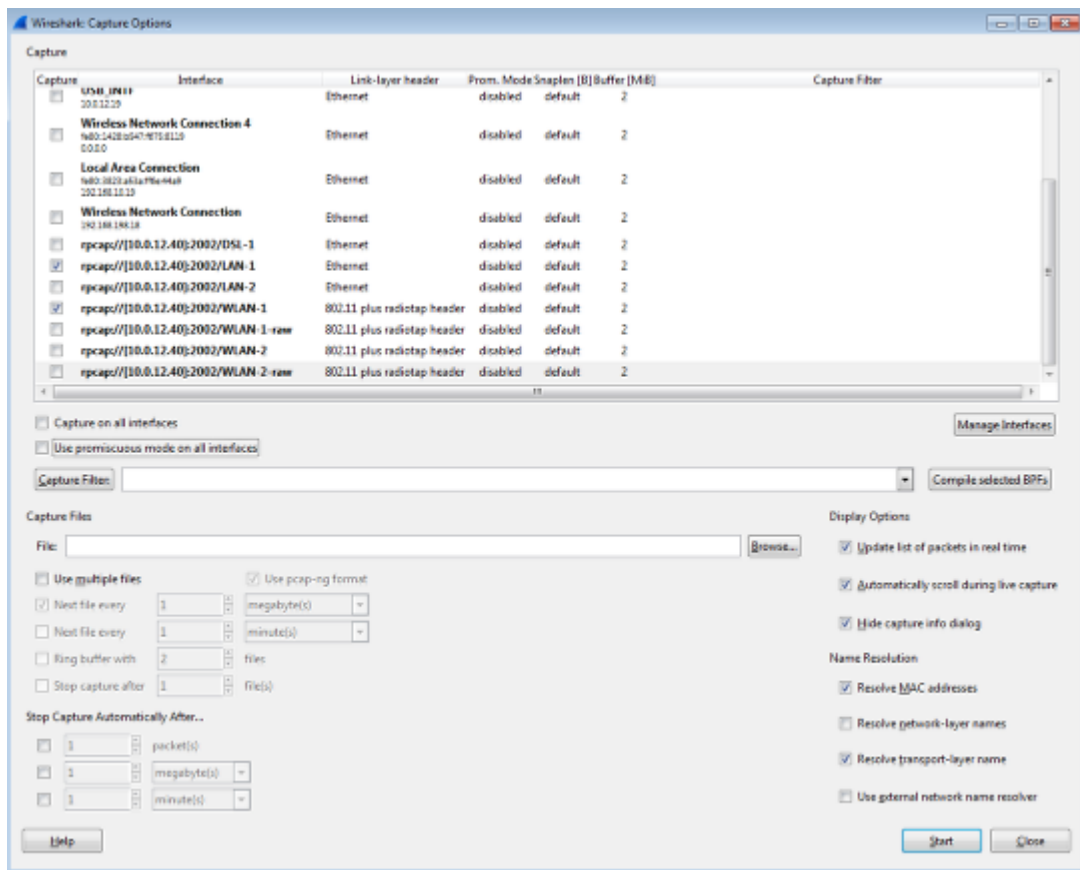
Give the IP address of the BAT, the RCap port relevant username and password to access the device then click ok

### RCap gives all the available interfaces on the remote device



click on Apply and Close

**From the Capture option Window, the remote interfaces are now available, select the one(s) you want to capture the traffic on.**



In this example traffic going through LAN-1 and WLAN-1 will be captured. Then just clic on start

## Result view

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets with columns for No., Time, Date, Source, Destination, Protocol, and Info. The bottom pane shows the details of the selected packet (No. 6), which is a RadioTap frame. The details include the RadioTap header, MAC timestamp, flags, data rate, channel frequency, and channel type. The packet is identified as an IEEE 802.11 Beacon frame.

| No. | Time        | Date                          | Source            | Destination | Protocol | Info                                     |
|-----|-------------|-------------------------------|-------------------|-------------|----------|--|
| 1   | 0.000000000 | 2016-02-07 07:34:42.124451000 | 10.0.12.40        | 10.0.12.19  | TCP      | mailbox > tdsos190 [ACK] Seq=1 Ack=1     |
| 2   | 0.000477000 | 2016-02-07 07:34:42.125130000 | 10.0.12.19        | 10.0.12.40  | TCP      | mosaicssysvcl > globe [ACK] Seq=1 Ack=1  |
| 3   | 0.001054000 | 2016-02-07 07:34:42.125707000 | 10.0.12.40        | 10.0.12.19  | TCP      | globe > mosaicssysvcl [ACK] Seq=1 Ack=1  |
| 4   | 0.002523000 | 2016-02-07 07:34:42.127174000 | 10.0.12.19        | 10.0.12.40  | TCP      | [TCP Previous segment not captured]      |
| 5   | 0.037883000 | 2016-02-07 07:34:42.162536000 | JuniperN_72:9b:00 | Broadcast   | 802.11   | Beacon frame, S=618, P=0, Flags=...      |
| 6   | 0.040730000 | 2016-02-07 07:34:42.165381000 | JuniperN_72:9b:04 | Broadcast   | 802.11   | Beacon frame, S=620, P=0, Flags=...      |
| 7   | 0.047596000 | 2016-02-07 07:34:42.172410000 | Sensoint_87:2d:ba | Broadcast   | 802.11   | Beacon frame, S=1027, P=0, Flags=...     |
| 8   | 0.052454000 | 2016-02-07 07:34:42.177107000 | JuniperN_72:9b:00 | Broadcast   | 802.11   | Beacon frame, S=1067, P=0, Flags=...     |
| 9   | 0.053866000 | 2016-02-07 07:34:42.178529000 | JuniperN_72:9b:02 | Broadcast   | 802.11   | Beacon frame, S=1068, P=0, Flags=...     |
| 10  | 0.063072000 | 2016-02-07 07:34:42.177721000 | 10.0.12.40        | 10.0.12.19  | TCP      | [TCP Acksed unseen segment] globe > m... |
| 11  | 0.003442000 | 2016-02-07 07:34:42.128095000 | 10.0.12.40        | 10.0.12.19  | RPCAP    | update filter reply                      |
| 12  | 0.003595000 | 2016-02-07 07:34:42.128244000 | 10.0.12.40        | 10.0.12.19  | TCP      | [TCP window update] globe > mosaicssy... |
| 13  | 0.038126000 | 2016-02-07 07:34:42.162779000 | 10.0.12.40        | 10.0.12.19  | RPCAP    | Packet                                   |
| 14  | 0.055322000 | 2016-02-07 07:34:42.179975000 | JuniperN_72:9b:04 | Broadcast   | 802.11   | Beacon frame, S=2069, P=0, Flags=...     |
| 15  | 0.055614000 | 2016-02-07 07:34:42.180267000 | 10.0.12.40        | 10.0.12.19  | RPCAP    | Packet                                   |
| 16  | 0.057542000 | 2016-02-07 07:34:42.182195000 | 10.0.12.19        | 10.0.12.40  | TCP      | brvcontrol > brutus [ACK] Seq=1 Ack=1    |
| 17  | 0.057810000 | 2016-02-07 07:34:42.182463000 | 10.0.12.40        | 10.0.12.19  | RPCAP    | Packet                                   |
| 18  | 0.059263000 | 2016-02-07 07:34:42.183916000 | Hirschma_ff:d2:f3 | Broadcast   | 802.11   | Beacon frame, S=1092, P=0, Flags=...     |
| 19  | 0.089998000 | 2016-02-07 07:34:42.214651000 | Hirschma_ff:d2:f3 | Broadcast   | 802.11   | Beacon frame, S=1404, P=0, Flags=...     |
| 20  | 0.112718000 | 2016-02-07 07:34:42.237371000 | Hirschma_ff:d3:04 | Broadcast   | 802.11   | Beacon frame, S=2869, P=0, Flags=...     |
| 21  | 0.141242000 | 2016-02-07 07:34:42.265795000 | JuniperN_72:9b:00 | Broadcast   | 802.11   | Beacon frame, S=824, P=0, Flags=...      |
| 22  | 0.141524000 | 2016-02-07 07:34:42.267110000 | JuniperN_72:9b:00 | Broadcast   | 802.11   | Beacon frame, S=824, P=0, Flags=...      |

Frame 6: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits) on interface 1  
 RadioTap Header v0, Length 36  
 Header revision: 0  
 Header pad: 0  
 Header length: 36  
 Present flags  
 MAC timestamp: 383751312  
 Flags: 0x00  
 Data rate: 2.0 Mb/s  
 Channel frequency: 2462 [66 11]  
 Channel type: 802.11g (pure-g) (0x00c0)  
 SSI signal: -57 dbm  
 SSI noise: -87 dbm  
 Antenna: 0  
 Channel number: 11  
 Channel frequency: 2462  
 Channel type: unknown (0x00400c0)  
 IEEE 802.11 Beacon frame, #Tags: 1  
 IEEE 802.11 Wireless LAN management frame

0000 00 20 24 50 8f 58 04 00 30 7a d8 18 05 50 00 04 ...  
 0010 04 04 9e 09 c0 00 c7 a9 00 00 00 00 c0 00 04 00 ...  
 0020 0e 09 0b 50 80 00 00 00 ff ff ff ff ff ff 3c 94 ...  
 0030 10 12 9b 04 31 84 d5 72 9b 04 c0 26 f9 50 77 03 ...  
 0040 0e 00 05 50 84 50 31 84 00 0a 42 47 57 2d 4e 8f ...  
 0050 0e 50 6c 75 01 0a 87 70 00 0a 42 47 57 2d 4e 8f ...

Packets: 1229 - Displayed: 1229 (100.0%) - Dropped: 5 (0.4%)

RPCap tunnels the traffic between the BAT and the capturing station. Packets from WLAN-1 with radio header and packets from LAN-1 are in the same capture but can be read separately filtering the interface id.