Marama QuickStart Guide

Marama.WiresharkUtility.QS.001.v0.10

Quick Start Guide
For
Wireshark Zigbee Sniffer Utility

DOCUMENT INFORMATION

Issued by: Jakob Bo Thomsen

Marama

Contact information

E-mail: jakob.thomsen@marama.dk

Copyless

Document updates

Revision	Date	Author	Change description
0.10	13/01/2010	JBT	Template and absolute minimum introduction to getting the utility running under Windows.

Table of Contents

Open and outstanding issues

#	Actionee	Issue	Details
1	JBT	Linux support	Describe how to use the Wireshark Zigbee utility under Linux
2	JBT	Wireshark and Zigbee	Describe how to monitor Zigbee traffic using Wireshark and the Wireshark Zigbee utility
3	JBT	Background	Add backuground information, e.g. Zigbee 101 and description of Exegin plugins / Zigbee decodes

1 Quick start guide to using the Zigbee Utility for Wireshark

1.1 Introduction

TBD:

<Simple program to support Wireshark Zigbee sniffer using a named pipe

- Wrapper: Freescale MC1322x USB dongle virtual serial port

- Wrapper: libpcap file format

- Main program

>

1.2 Using the utility program with Wireshark (Windows platform)

Pre-requisites:

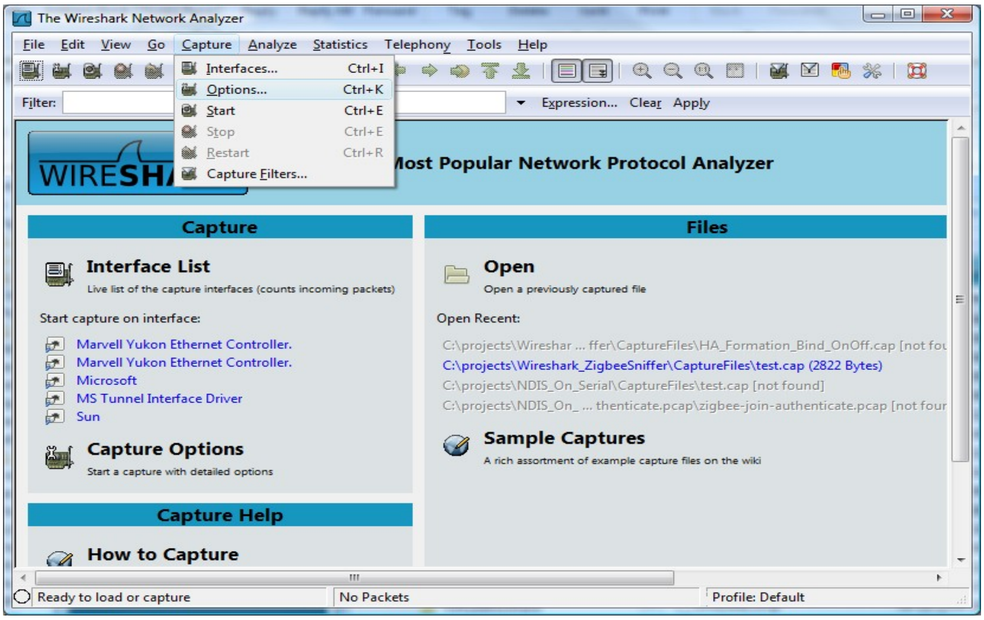
1) You have downloaded the latest Wireshark Zigbee utility zip file from Sourceforge
2) You have already installed Wireshark version 1.20 or later (incl. basic Zigbee message decoding)
3) You have a Freescale MC1322x USB dongle attached and the virtual serial port driver installed

Instructions:

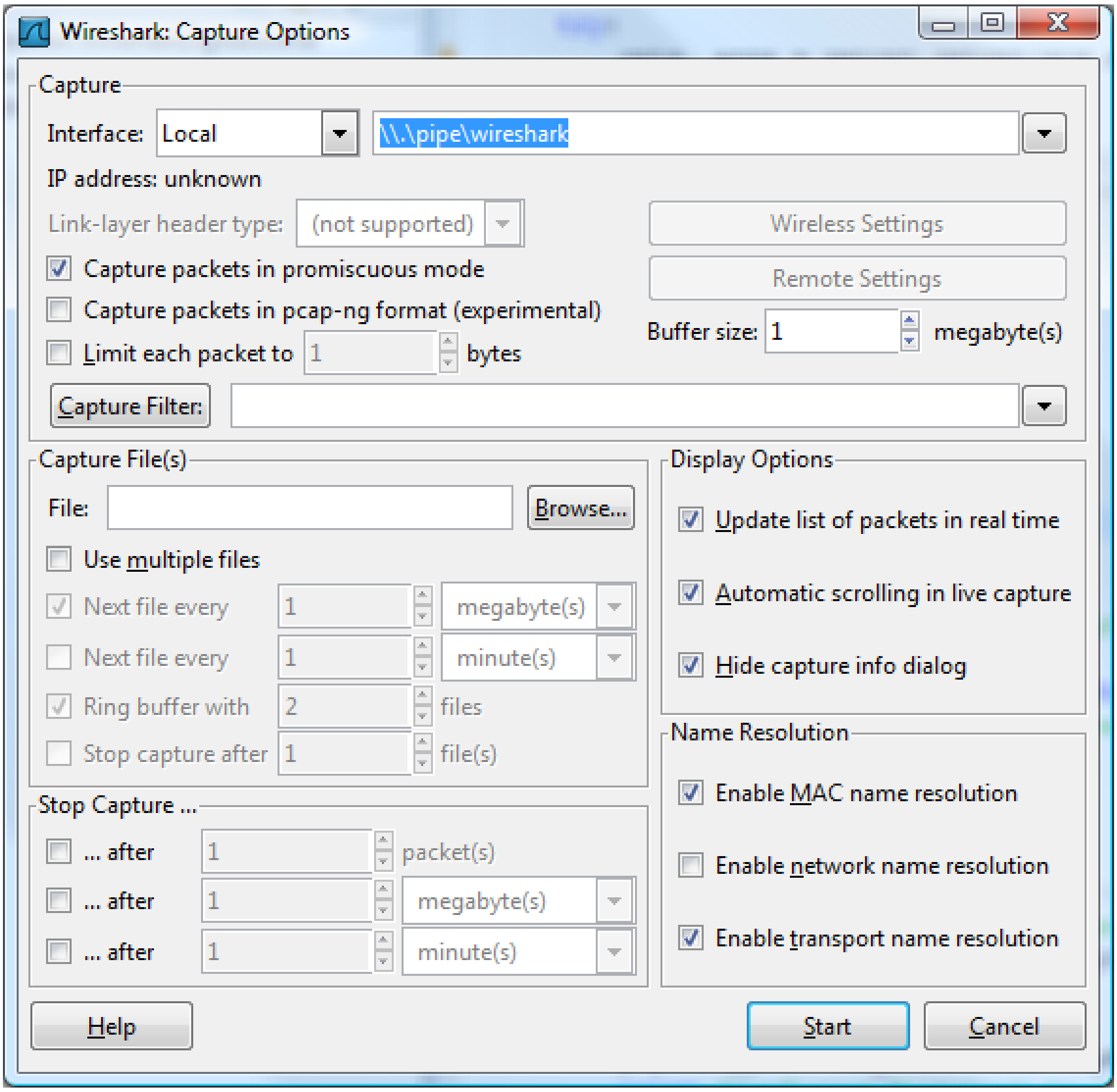
1) Unzip the zip file and open a command prompt (DOS box) in the directory where the files where unzipped
2) Start the utility, specififying the serial port and channel to monitor:

```
c:\path>WS_ZigbeeSnifferUtility.exe -port=COM8 -channel=14
Configuring sniffer on port 'COM8' to listen on channel 14
Configure Wireshark to listen to the name pipe '\\.\pipe\wireshark'
```

3) Copy the pipe name '\\.\pipe\wireshark' to the clipboard
4) Start Wireshark and open the Capture ¦ Options dialog:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Filter:
Expression... Clear Apply
WIRESHA
Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Marvell Yukon Ethernet Controller.
Marvell Yukon Ethernet Controller.
Microsoft
MS Tunnel Interface Driver
Sun
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Files
Open
Open a previously captured file
Open Recent:
C:\projects\Wireshar ... ffer\CaptureFiles\HA_Formation_Bind_OnOff.cap [not fou
C:\projects\Wireshark_ZigbeeSniffer\CaptureFiles\test.cap (2822 Bytes)
C:\projects\NDIS_On_Serial\CaptureFiles\test.cap [not found]
C:\projects\NDIS_On_ ... thenticate.pcap\zigbee-join-authenticate.pcap [not four
Sample Captures
A rich assortment of example capture files on the wiki
Ready to load or capture
No Packets
Profile: Default

5) Paste the pipe name in the local interface name:



Capture

Interface: Local \\.\pipe\wireshark

IP address: unknown

Link-layer header type: (not supported)

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter:

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

6) Press 'Start' and you should be sniffing.

1.3 Using the utility program with Wireshark (Linux platform)

TBD

2 Analysing Zigbee Traffic using Wireshark

TBD:

- Sample setup, Zigbee network, Sniffer setup
- Sample scenario
- Sample capture

(Security)

3 Background

TBD:

- Zigbee mesh networks
- Wireshark as a Zigbee analyser, Exegin, v1.20++
- Network adapter vs. named pipe

4 Appendix: Terms and Definitions

TBD

5 Appendix: References

TBD