# PANalyzr<sup>™</sup> SW Install Procedure for Windows

01/07/2022

# Table of Contents

| v0.9.0 PANalyzr Release Notes                | 2 |
|--|---|
| Spanalytics Contact Details                  | 3 |
| Open-Source Utilities                        | 3 |
| Introduction4                                | 1 |
| System Requirements4                         | ļ |
| Remove PANalyzr v0.8.1 Wireshark plugin4     | ļ |
| Install Wireshark & Npcap4                   | ļ |
| Uninstall any previous version of PANalyzr11 | L |
| Install the PANalyzr Software11              | L |
| Install Python14                             | 1 |
| Z-Wave Packet Capturing Setup17              | 7 |
| Pyserial and bitstring python packages17     | 7 |
| Install the z-wave sniffing python scripts17 | 7 |
| Z-Wave driver                                | 7 |
| 12 A A A A A A A A A A A A A A A A A A A     |   |
| Install Oser License                         | 7 |

# v0.9.0 PANalyzr Release Notes

#### 01/07/2022

#### **New Features**

- > Hardware Control Interface (HCI) packet capturing in Wireshark
- Improved meta data display
- Improved graph displays: RSSI over hits (piconet traffic) and scatter plot of RF channel over hits (piconet traffic)
- > Added several pre-configured filters for use on Wireshark startup
- > Upgraded Bluetooth and Z-Wave plugins to work with Wireshark version 3.6.0
- Message Sequencing Chart view for Bluetooth packets (in Wireshark)
- PANalyzr-IoT Expansion Pack Z-Wave, 802.15.4 (2.4GHz and Sub-GHz) and Wi-Fi packet capturing, including channel, frequency, and modulation selection options
- > Z-Wave, Bluetooth BR/EDR and 802.15.4 Data Export capability
- Process BR/EDR Secure Connections encrypted packets (includes new MIC field in the Wireshark dissection)
- Show BR/EDR Null and Poll packets
- > BR/EDR packet identification improvement
- Find-IT now also for 802.15.4
- New FindIT gauge view
- New GUI controls to run Brackle from the PANalyzr application (Windows command prompt no longer needed)
- Improved Brackle runtime performance
- Indicate the Source and Destination address of every Bluetooth BR/EDR packet in the Wireshark packet data
- Indicate the Peripheral address value of a connection in the Bluetooth BR/EDR packet header data
- > Auto launcher to start or stop PANalyzr software at user-set date or time
- Display PANalyzr-IoT hardware status on startup
- Sample BLE, BREDR, and PANalyzr-IoT capture files included with the installation
- PANalyzr-IoT profile including useful columns for all protocols

#### **Bug Fixes**

- Add channels 12, 13, 14 to the Wi-Fi Channel Sweep list
- > Fix for default PANalyzr config .json file path
- > Fix for Brackle crash if a file or folder with a space character is used
- Fix for BLE packet timestamps aren't reset between captures
- > Fix for Brackle crashes when invalid parameters are used
- Fix for Wi-Fi capturing does not stop when using dumpcap
- Fix for FindIT angle deg value does not update
- Various software crash fixes and improved stability

Page 2 of 17

# Spanalytics Contact Details

Technical Support: <u>support@panalyzr.com</u> Technical Support Phone: 804-364-1050, option 6

Sales: <a href="mailto:sales@panalyzr.com">sales@panalyzr.com</a>

Other inquiries: <a href="mailto:support@panalyzr.com">support@panalyzr.com</a>

# **Open-Source Utilities**

The PANalyzr protocol analyzer software uses the open-source utility Wireshark to provide additional features to the system. The modified binary is included in this installation, and the modified source code is available upon request.

- Knob The original Knob code can be found at <a href="https://github.com/francozappa/knob">https://github.com/francozappa/knob</a>. The source code modifications made are included in this installation (located in the C:\Program Files (x86)\Spanalytics\PANalyzr directory after the installation completes)
- □ E0 The original E0 code can be found at <u>https://github.com/adelmas/e0</u>. The source code modifications made for this installation are available upon request
- □ Brackle The original crackle code can be found at <u>https://github.com/mikeryan/crackle</u>. The source code modifications made for this installation are available upon request
- Wireshark The original Wireshark code can be found at <u>https://www.wireshark.org/download.html</u>. The source code modifications made for this installation are available upon request
- □ KillerZee The original code can be found at <u>https://github.com/joswr1ght/killerzee</u>. The source code modifications made for this installation are available upon request
- □ Z-Wave Wireshark plugin The original code can be found at <u>https://github.com/AFITWiSec/EZ-</u> <u>Wave</u>. The source code modifications for this installation are available upon request
- □ libpcap The original libpcap code can be found at <u>https://www.tcpdump.org/index.html#latest-releases</u>

## Introduction

This procedure describes the steps required to install and run the latest version of the PANalyzr protocol analyzer software on a Windows 10 machine.

#### System Requirements

The following system settings and software are recommended for the PANalyzr protocol analyzer software:

- Windows 10
- 20GB free hard drive space
- 8GB RAM
- Internet access (to download required package dependencies)

## Remove PANalyzr v0.8.1 Wireshark plugin

(The steps in this section are only applicable if PANalyzr v0.8.1 is installed on this computer)

- Open a Windows File Explorer Window
- □ Navigate to the Wireshark Global Plugins folder (by default, this folder is usually set to *C:\Program Files\Wireshark\plugins\3.4\epan*)
- □ Remove the file **panalyzr.dll** from this folder

## Install Wireshark & Npcap

PANalyzr requires Wireshark version 3.6.0 (or higher) and Npcap version 1.55 to be installed on the computer before running the PANalyzr installation, and some packet data will not be appropriately captured unless Wireshark and Npcap are installed as described in this section.

Additionally, the process used to install a newer version of Wireshark on the computer could remove existing Wireshark preferences and configuration files. A backup of these files is strongly recommended before installing/re-installing Wireshark

Download the latest version of Wireshark from <a href="https://www.wireshark.org/#download">https://www.wireshark.org/#download</a>



- Double-click on the Wireshark-win64-3.#.#.exe file
- □ In the "Welcome to Wireshark 3.6.0 64-bit Setup" window, click the **Next** button

| 🚄 Wireshark 3.6.0 64-bit Setup | X  |
|--------------------------------|--|
|                                | Welcome to Wireshark 3.6.0 64-bit<br>Setup                               |
|                                | This wizard will guide you through the installation of Wireshark.        |
|                                | Before starting the installation, make sure Wireshark is not<br>running. |
|                                | Click 'Next' to continue.  |
|                                | Next > Cancel  |

#### □ In the "License Agreement" window, click on the **Noted** button

| 🚄 Wireshark 3.6.0 64-bit Setup —  | ×   |
|---|-----|
| License Agreement   |     |
| Please review the license terms before installing Wireshark 3.6.0 64-bit.   |     |
| Wireshark is distributed under the GNU General Public License.  |     |
| This text consists of three parts:  | ^   |
| Part I: Some remarks regarding the license given in<br>Part II: The actual license that covers Wireshark.<br>Part III: Other applicable licenses.<br>When in doubt: Part II/III is the legally binding part, Part I is just<br>there to make it easier for people that are not familiar with the GPLv2. |     |
|   | ~   |
| This is not an end user license agreement (EULA). It is provided here for informational<br>purposes only.   |     |
| Wireshark® Installer  |     |
| < Back Noted Can  | tel |

 $\hfill\square$  In the "Choose Components" window, click on the **Next** button

| 🚄 Wireshark 3.6.0 64-bit Setup                      | – 🗆 X  |
|---|--|
| Choose Components<br>Choose which features of Wires | shark 3.6.0 64-bit you want to install.  |
| The following components are a                      | vailable for installation.   |
| Select components to install:                       | Wireshark      ···· ✔      Wireshark      ···· ✔      Plugins & Extensions      ···· ✔      Tools      ···· ✔      ···· ✔      Documentation |
| Space required: 223.4 MB                            | Description<br>Position your mouse over a component to see its<br>description.   |
| Wireshark® Installer ————                           | < Back Next > Cancel   |

□ In the "Additional Tasks" window, click on the **Next** button

| Wireshark 3.6.0 64-bit Setup   | _               |    | ×    |
|--|-----------------|----|------|
| Additional Tasks   |                 |    |      |
| Create shortcuts and associate file extensions.  |                 |    |      |
| Create Shortcuts   |                 |    |      |
|  |                 |    |      |
|  |                 |    |      |
| Wireshark Desktop Icon   |                 |    |      |
| Wireshark Quick Launch Icon  |                 |    |      |
| Associate File Extensions  |                 |    |      |
| Associate trace file extensions with Wireshark   |                 |    |      |
| Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix,<br>mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1,<br>trc, vwr, wpc, and wpz. | lcap,<br>trace, |    |      |
|  |                 |    |      |
| Wiesbark@Techallar   |                 |    |      |
| VVITESTIATING LISUALET   | >               | Ca | ncel |

□ In the "Choose Install Location" window, click on the **Next** button

| 🚄 Wireshark 3.6.0 64-bit Setup                                | -    |      | ×    |
|---|------|------|------|
| Choose Install Location                                       |      |      |      |
| Choose the folder in which to install Wireshark 3.6.0 64-bit. |      |      |      |
| Choose a directory in which to install Wireshark.             |      |      |      |
|   |      |      |      |
|   |      |      |      |
|   |      |      |      |
| Destination Folder  |      |      |      |
| C:\Program Files\Wireshark                                    | Bro  | owse |      |
| Space required: 223.4 MB                                      |      |      |      |
| Space available: 117.6 GB                                     |      |      |      |
| Wireshark® Installer  |      |      |      |
| < Back Nex  | xt > | Car  | ncel |

□ In the "Packet Capture" window, select the "Install Npcap #.##" box and click on the **Next** button

| p or Winf             | Pcap           |
|-----------------------|----------------|
|                       |                |
| the comm<br>n't crash | mand<br>nagain |
|                       |                |
|                       |                |
|                       |                |
|                       |                |
|                       |                |

□ In the "USB Capture" window, click on the Install button

| 🚄 Wireshark 3.6.0 64-bit Setup  | -           |           | ×   |
|---|-------------|-----------|-----|
| USB Capture   |             |           |     |
| USBPcap is required to capture USB traffic. Should USBPcap be install (experimental)?                               | led         |           |     |
| Currently installed USBPcap version   |             |           |     |
| USBPcap is currently not installed  |             |           |     |
| Install   |             |           |     |
| Install USBPcap 1.5.4.0   |             |           |     |
| (Use Add/Remove Programs first to uninstall any undetected o  | ld USBPcap  | versions) |     |
| Important notice  |             |           |     |
| In case of issue after installation, please use the system restore p<br>https://github.com/desowin/usbpcap/issues/3 | oint create | d or read |     |
|   |             |           |     |
| Learn more about USBPcap  |             |           |     |
|   |             |           |     |
| Wireshark® Installer  |             |           |     |
| < Back Ir   | nstall      | Cano      | tel |
|   |             |           |     |

□ In the "Npcap License Agreement" window, click the I agree button

| 🌍 Npcap 1.55 Setup   |   |  | _       |          | ×   |
|--|---|--|---------|----------|-----|
| NMAP, ORG  | License Agreement<br>Please review the license terr   | ms before instal                                       | ling Np | cap 1.55 |     |
| Press Page Down to see the   | e rest of the agreement.  |  |         |          |     |
| NPCAP COPYRIGHT / END  | USER LICENSE AGREEMENT  |  |         |          | ^   |
| Npcap is a Windows packe<br>(c) 2013-2021 by Insecure<br>reserved.   | t sniffing driver and library and i<br>.Com LLC ("The Nmap Project")  | is copyright<br>. All rights                           |         |          |     |
| Even though Npcap source<br>not open source software<br>permission from the Nmap<br>limited to installation on fiv | code is publicly available for re<br>and may not be redistributed wi<br>Project. The standard version i<br>e systems. We fund the Npcap | view, it is<br>ithout special<br>is also<br>project by |         |          | Ŷ   |
| If you accept the terms of agreement to install Npcap  | the agreement, click I Agree to 1.55.   | continue. You m  | nust ac | cept the |     |
| Nullsoft Install System v3.07 -  |   |  |         |          |     |
|  |   | I Agree  |         | Cano     | cel |

□ In the "Installation Options" window, select the "Support raw 802.11 traffic..." and the "Install Npcap in WinPcap..." boxes, and click the **Install** button

| 🌐 Npcap 1.55 Setup              |  |                              |              | _        |           | ×   |
|---------------------------------|--|------------------------------|--------------|----------|-----------|-----|
| NMAP. ORG                       | Installation Option<br>Please review the | <b>ns</b><br>following optio | ns before in | stalling | ) Npcap 1 | .55 |
|                                 |  |                              |              |          |           |     |
| Restrict Npcap drive            | r's access to Administ                   | rators only                  |              |          |           |     |
| Support raw 802.11              | traffic (and monitor n                   | node) for wirel              | ess adapter  | s        |           |     |
| 🗹 Install Npcap in WinF         | Pcap API-compatible N                    | 1ode                         |              |          |           |     |
|                                 |  |                              |              |          |           |     |
|                                 |  |                              |              |          |           |     |
|                                 |  |                              |              |          |           |     |
|                                 |  |                              |              |          |           |     |
| Nullsoft Install System v3.07 - |  |                              |              |          |           |     |
|                                 | [  | < Back                       | Install      |          | Cano      | el  |

□ In the "Installation Complete" window, click the **Next** button after the installation is complete.

| 🌐 Npcap 1.55 Setup   |  | _     |      | $\times$ |
|--|--|-------|------|----------|
| NMAP. ORG  | Installation Complete<br>Setup was completed successfully.   |       |      |          |
| Completed  |  |       |      |          |
|  |  |       |      |          |
| Npcap WFP callout driver<br>Installing NDIS filter drive<br>Npcap LWF driver (with V<br>The npcap service was su<br>Writing service options to<br>Starting the npcap driver<br>Output folder: C: \Progra<br>Extract: CheckStatus.bal<br>Creating npcapwatchdog | has been successfully installed!<br>r<br>Vi-Fi support) has been successfully install<br>uccessfully created<br>o registry<br>m Files\Npcap<br>t<br>scheduled task | ed!   |      | ^        |
| Completed  |  |       |      | ~        |
| Nullsoft Install System v3.07 -  | < Back N   | ext > | Cano | cel      |

#### □ In the "Finished" window, click the **Finish** button

| 🌐 Npcap 1.55 Setup              |  | _      |       | $\times$ |
|---------------------------------|--|--------|-------|----------|
| NMAP. ORG                       | Finished<br>Thank you for installing Npcap |        |       |          |
| Npcap has been installe         | d on your computer.                        |        |       |          |
| Click Finish to close this      | wizard.                                    |        |       |          |
|                                 |  |        |       |          |
|                                 |  |        |       |          |
|                                 |  |        |       |          |
|                                 |  |        |       |          |
|                                 |  |        |       |          |
| Nullsoft Install System v3.07 - |  |        |       |          |
|                                 | < <u>B</u> ack                             | Finish | Cance | el       |

□ In the "Wireshark Installation Complete" window, click the **Next** button



□ In the "Completing Wireshark 3.4.7 64-bit Setup" window, click the **Finish** button.

| <u> (</u> Wireshark 3.6.0 64-bit Setup | - 🗆 ×   |  |  |  |  |  |
|--|---|--|--|--|--|--|
|  | Completing Wireshark 3.6.0 64-bit<br>Setup  |  |  |  |  |  |
|  | Wireshark 3.6.0 64-bit has been installed on your computer.<br>Click Finish to close Setup. |  |  |  |  |  |
|  | Show News   |  |  |  |  |  |
|  | < Back Finish Cancel  |  |  |  |  |  |

## Uninstall any previous version of PANalyzr

□ Using the Windows Control Panel, uninstall any previous version(s) of PANalyzr software

## Install the PANalyzr Software

The steps below should take approximately 3 minutes to complete, depending on how many of the required packages are already installed on the machine

- Download the **PANalyzr\_Setup.exe** to the desired location on the local machine
- Double-click the **PANalyzr\_Setup.exe** to initiate the install process

□ The *Welcome to the Wizard for PANalyzr Setup* window will open and begin the installation process. Select the **Next** button to continue the installation



□ The "Spanaytics, LLC End-User License Agreement" will be displayed in a scroll box on the PANalyzr Installshield Wizard window. Scroll through the "Spanaytics, LLC End-User License Agreement" to view the agreement documentation.



Page 12 of 17

- □ Select the 'I accept the terms in the license agreement' radio button
- □ Click the **Next** button in the *PANalyzr Wizard* window dialog window to continue the installation
- □ The proposed 'Destination Folder' for the application install is displayed, with a button option to change the directory. Select the desired directory or make no changes to accept the default directory. Click the **Next** button to continue the installation



□ The *PANalyzr Wizard* will prompt for the **Microsoft Visual C++ 2015-2019 Redistributable (x86)** - **14.26.28720**, if it's not installed

| Microsoft Visual C++ 2015-2019  |   |  |  |  |  |
|---|---|--|--|--|--|
|   |   |  |  |  |  |
| Redistributable (x86) - 14.26.28720   |   |  |  |  |  |
| MICROSOFT SOFTWARE LICENSE TERMS  | ^ |  |  |  |  |
| MICROSOFT VISUAL C++ 2019 RUNTIME   |   |  |  |  |  |
| These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. They apply to the software named above. The terms also apply to any Microsoft services or |   |  |  |  |  |
| I agree to the license terms and conditions   |   |  |  |  |  |
| Close Close   |   |  |  |  |  |

During the install a popup 'User Account Control' window may be displayed, prompting the user to allow the app to make changes to the device. Click the Yes button to continue

## Install Python

The Z-wave packet capturing and the Brackle packet decryption utilities both require Python. For both functions to work correctly, Python must be installed as described in this section.

□ In the "Install Python 3.9.2 (64-bit)" window, check the "Add Python 3.9 to PATH" checkbox and click the **Customize installation** text



□ In the "Optional Features" window, select the "Python test suite" box and click the **Next** button

| Python 3.9.2 (64-bit) Setup |   | -      |         | ×  |
|-----------------------------|---|--------|---------|----|
|                             | Optional Features   |        |         |    |
|                             | Documentation   |        |         |    |
| 9                           | ✓ pip<br>Installs nin, which can download and install other Put!  | hon na | ckages  |    |
|                             | Installs pip, when can download and install other ryd<br>I td/tk and IDLE<br>Installs tkinter and the IDLE development environmer | nt.    | crages. |    |
|                             | ✓ Python test suite<br>Installs the standard library test suite.  |        |         |    |
|                             | ☑ py launcher ☑ for all users (requires elevation)<br>Use Programs and Features to remove the 'py' launch                         | her.   |         |    |
| python                      |   |        |         |    |
| wind <mark>ows</mark>       | Back  | t      | Cano    | el |

- □ In the "Advanced Options" window, select the "Precompile standard library," "Download debugging symbols," and the "Download debug binaries.." boxes.
- □ Next, enter the following text in the "Customize install location" field: C:\Python39
- □ Click the **Install** button

| 눩 Python 3.9.2 (64-bit) Setup |  | -     |       | × |
|-------------------------------|--|-------|-------|---|
|                               | Advanced Options                                       |       |       |   |
|                               | ☑ Install for all users                                |       |       |   |
|                               | Associate files with Python (requires the py launcher) |       |       |   |
| _                             | Create shortcuts for installed applications            |       |       |   |
|                               | Add Python to environment variables                    |       |       |   |
|                               | Precompile standard library                            |       |       |   |
|                               | Download debugging symbols                             |       |       |   |
|                               | Download debug binaries (requires VS 2017 or later)    |       |       |   |
|                               | Customize install location                             |       |       |   |
|                               | C:\Python39  |       | Brows | e |
| python                        |  |       |       |   |
| for                           |  |       |       |   |
| WINDOWS                       | Back   | ill 👘 | Cance | 4 |
|                               |  |       |       |   |

Page 15 of 17

□ The PANalyzr installation continues, and the 'InstallShield Wizard Completed' message is displayed when the install is complete. Click the **Finish** button to close the 'PANalyzr Wizard' window



# Z-Wave Packet Capturing Setup

#### Pyserial and bitstring python packages

- Open a Windows command prompt window
- Install the pyserial package by typing the following at the command prompt:
  py -m pip install pyserial
- □ Install the bitstring package by typing the following at the command prompt: pip3 install bitstring

#### Install the z-wave sniffing python scripts

- Open a Windows command window with *administrator* privileges
- □ At the command prompt type: cd C:\Program Files (x86)\Spanalytics\PANalyzr\zwave\_sniffer
- □ Install the zwave sniffer software by typing the following at the command prompt: **python** setup.py install

This will install the zwave\_sniffer packages needed for the zwdumppcap.py script to execute.

#### Z-Wave driver

The Z-wave hardware requires a driver. It can be found in the **ZW050x\_USB\_VCP\_PC\_Driver** folder in the newly created **PANalyzr** folder. Follow the steps to install the driver.

- □ Open a Window File Explorer Window and navigate to the folder C:\Program Files(x86)\Spanalytics\PANalyzr\zwave\_sniffer\ZW050x\_USB\_VCP\_PC\_Driver
- □ Install the UZB driver by right-clicking on the **uzb.inf** file and choosing **Install**
- □ Plugin the Z-wave sniffer dongle

### Install User License

□ Copy the provided \*.pbk and \*.lic files to the selected PANalyzr software installation folder (the default installation path is C:\Program Files (x86)\Spanalytics\PANalyzr)

## Run PANalyzr

See the PANalyzr User Guide for details on how to utilize the PANalyzr protocol analyzer hardware and software.