PANalyzr™ SW Install Procedure for Windows

11/17/2022

Table of Contents

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

v0.9.9.3 PANalyzr Release Notes

New features

- Added new In-Place Monitoring System (IPMS) data view
- New BLE categorization status and colorization in metadata (approved/not approved/uncategorized)
- WIDS – Add First Seen and Last Seen columns in BLE metadata
- Added delete capture file capability
- Include new TSCH (Zigbee) and dual-band (WiSUN) Q59L firmware .dfu files with the installer
- Add User Guide to PANalyzr GUI Help menu
- Add clearer message for panalyzr.dll copy failure (Windows)

Bug Fixes

- SDR capture options become enabled when no SDR is attached
- Include the latest User Guide and Install Procedure in the installation folder
- 802.15.4 metadata tab is not displayed if the IoT EP license is not enabled
- Fixed overlapping pop-up dialogs box on the BLE metadata tab
- "Run-Time Check Failure #2" error was raised when using the GPS

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

Spanalytics Contact Details

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

Sales: sales@panalyzr.com

Other inquiries: support@panalyzr.com

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 https://github.com/francozappa/knob. 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 https://github.com/adelmas/e0. The source code modifications made for this installation are available upon request
- ☐ Brackle – The original crackle code can be found at https://github.com/mikeryan/crackle. The source code modifications made for this installation are available upon request
- ☐ Wireshark – The original Wireshark code can be found at https://www.wireshark.org/download.html. The source code modifications made for this installation are available upon request
- ☐ KillerZee – The original code can be found at https://github.com/joswr1ght/killerzee. The source code modifications made for this installation are available upon request
- ☐ Z-Wave Wireshark plugin – The original code can be found at https://github.com/AFITWiSec/EZ-Wave. The source code modifications for this installation are available upon request
- ☐ libpcap – The original libpcap code can be found at https://www.tcpdump.org/index.html#latest-releases

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

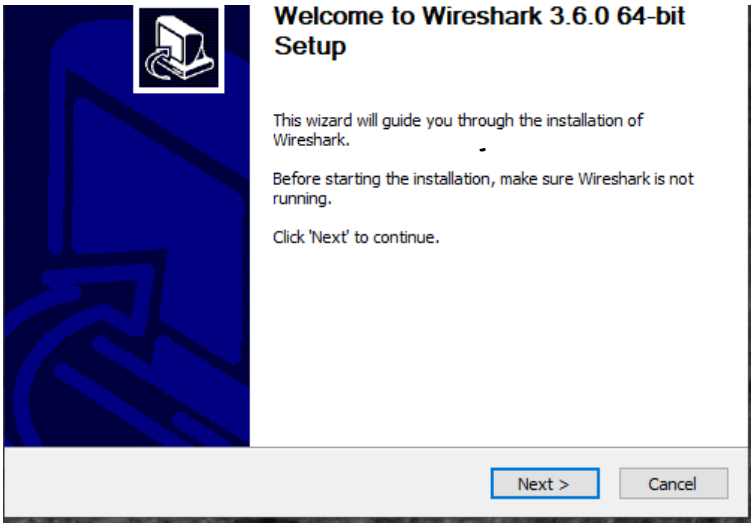
PANalyzr requires Wireshark version 3.6.8 and Npcap version 1.60 to be installed on the computer before running the PANalyzr installation. As described in this section, some packet data will not be appropriately captured unless Wireshark and Npcap are installed.

Additionally, installing 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

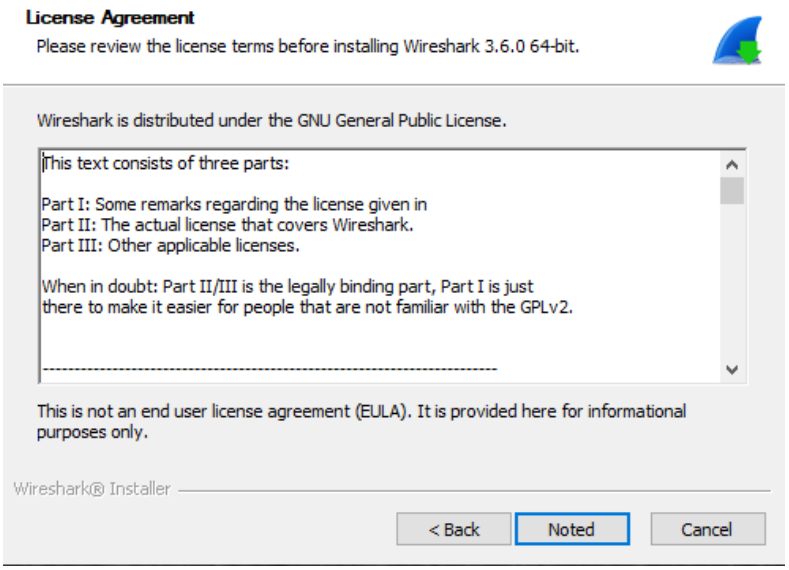
- ☐ Download version 3.6.# of Wireshark from https://www.wireshark.org/#download

- ☐ Double-click on the **Wireshark-win64-3.#.#.exe** file
- ☐ In the "Welcome to Wireshark 3.6.# 64-bit Setup" window, click the **Next** button

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

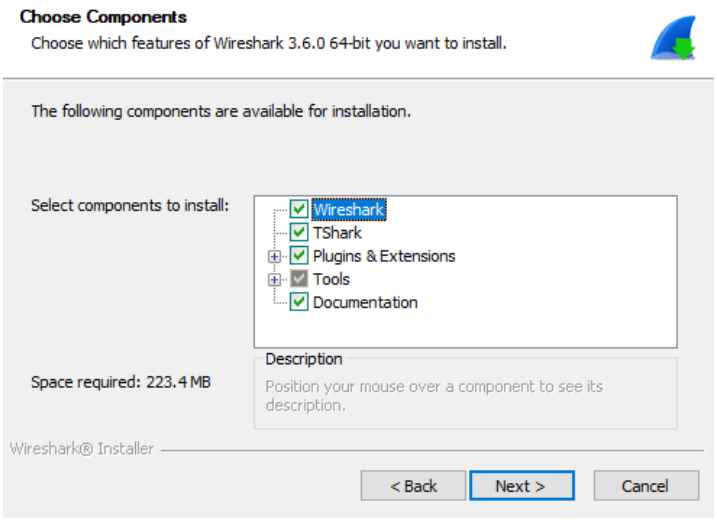


☐ In the “License Agreement” window, click on the **Noted** button

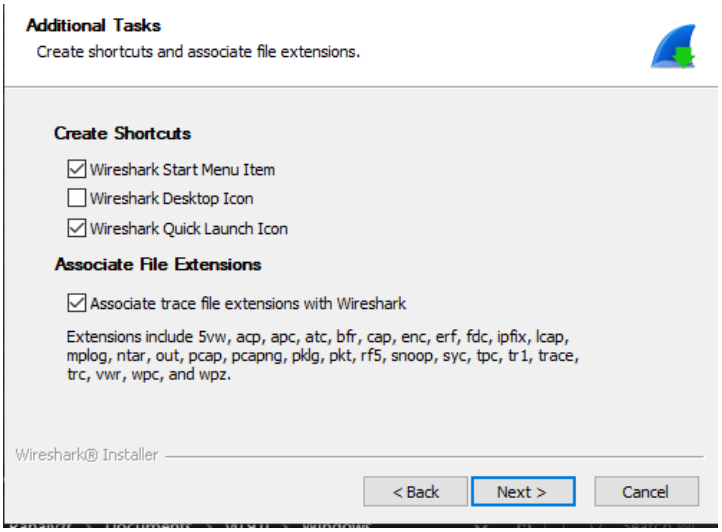


☐ In the “Choose Components” window, click on the **Next** button

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

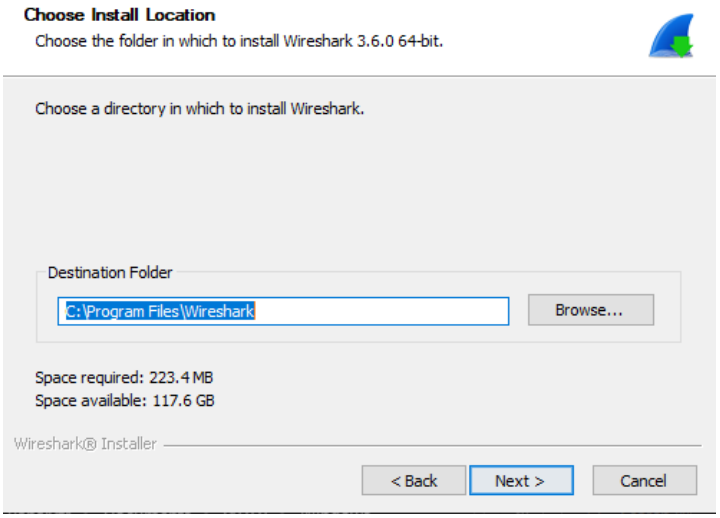


☐ In the "Additional Tasks" window, click on the **Next** button

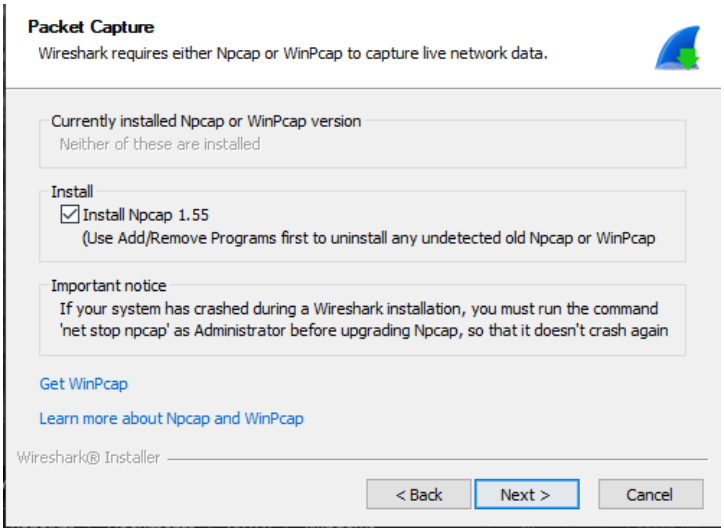


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

☐ In the “Choose Install Location” window, click on the **Next** button

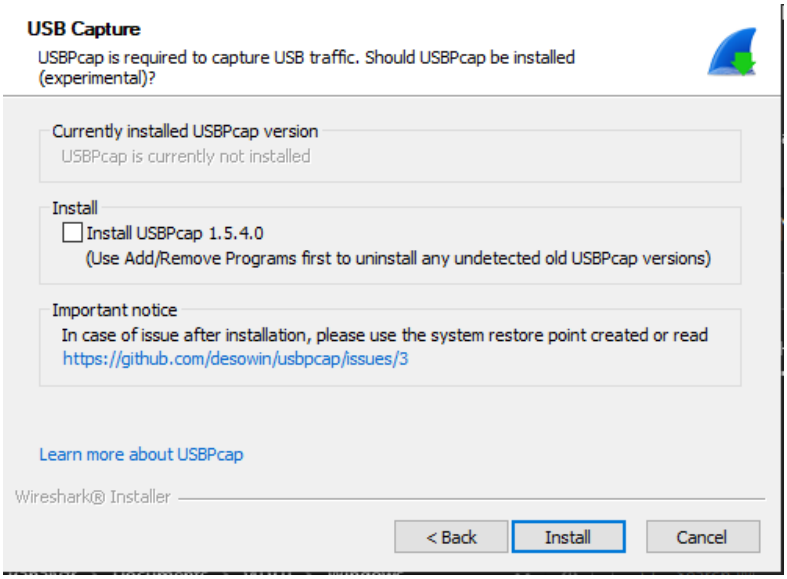


☐ In the “Packet Capture” window, select the “Install Npcap #.##” box and click on the **Next** button

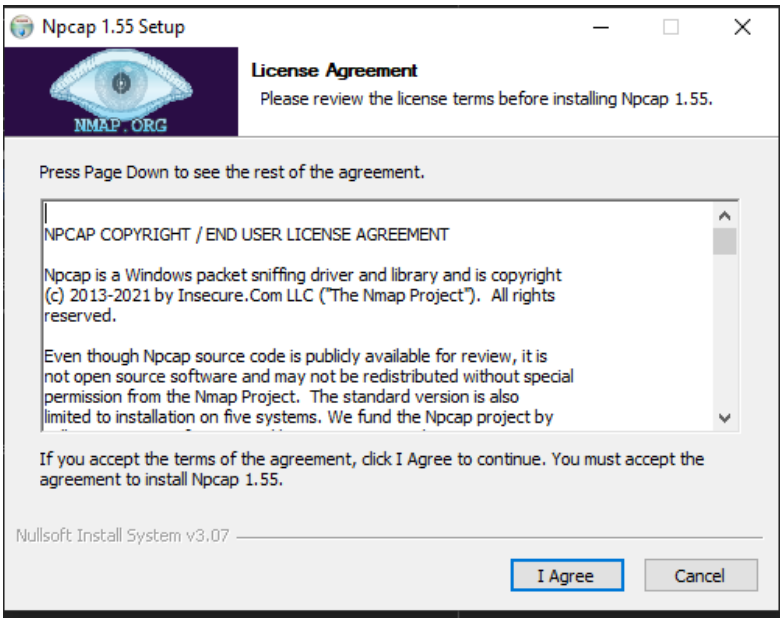


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

☐ In the “USB Capture” window, click on the **Install** button

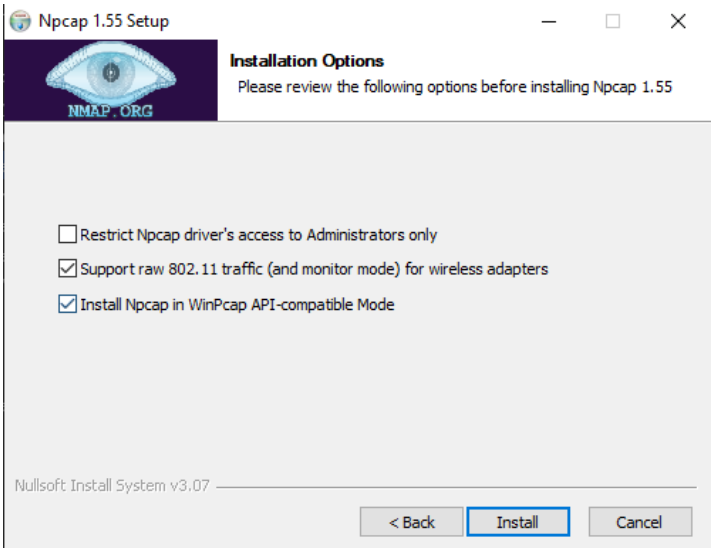


☐ In the “Npcap License Agreement” window, click the **I agree** button

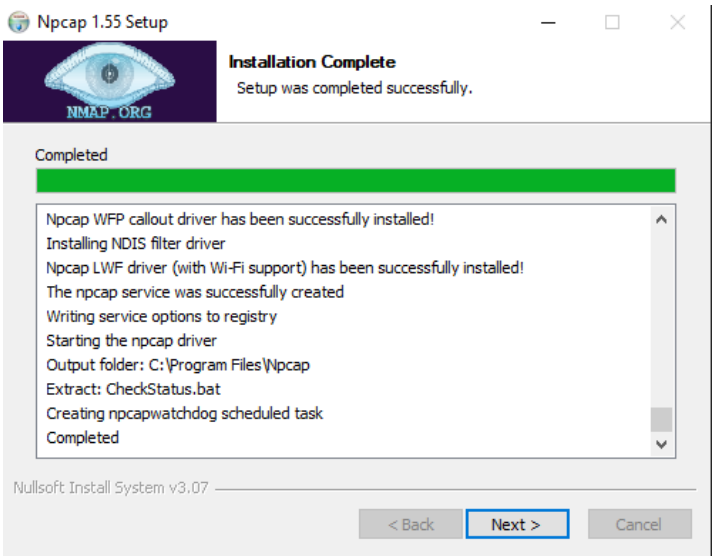


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

☐ In the “Installation Options” window, select the “Support raw 802.11 traffic…” and the “Install Npcap in WinPcap…” boxes, and click the **Install** button

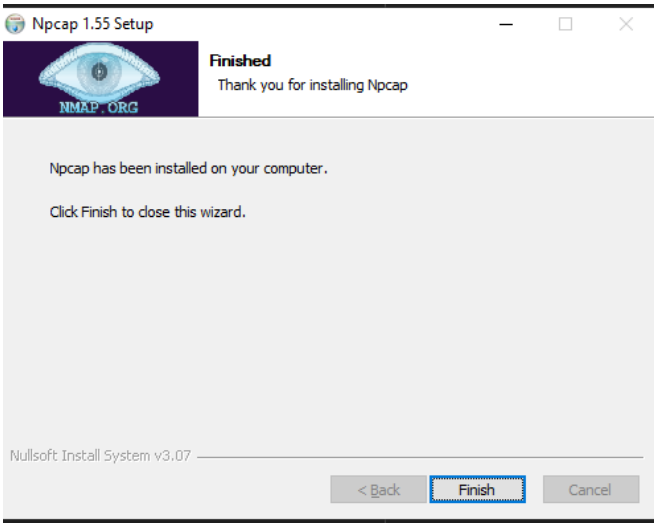


☐ In the “Installation Complete” window, click the **Next** button after the installation is complete.

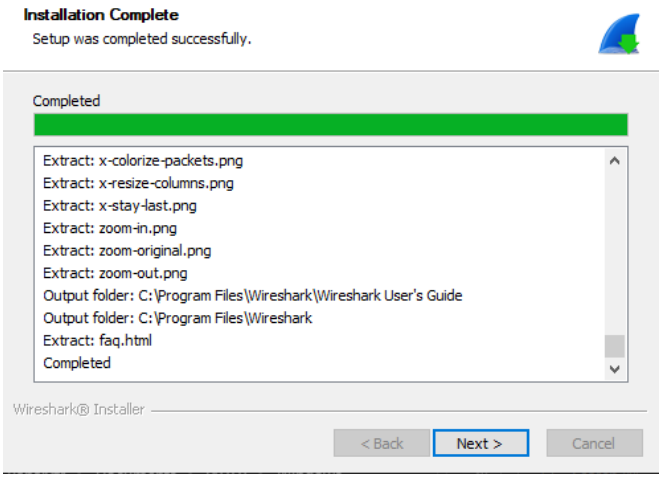


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

☐ In the “Finished” window, click the **Finish** button

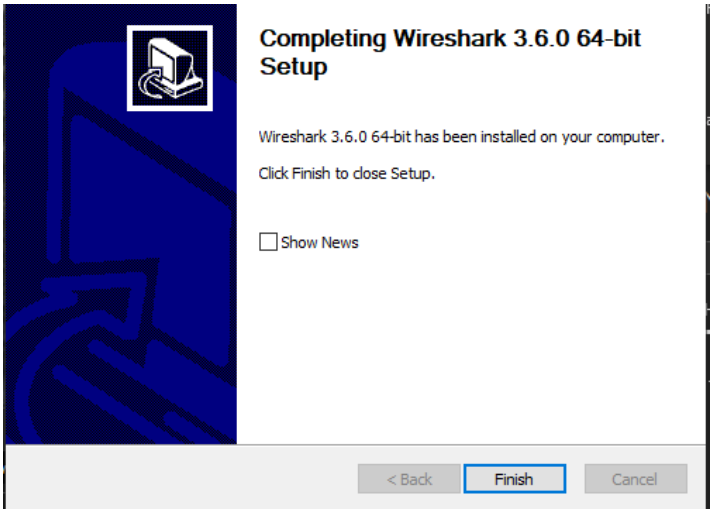


☐ In the “Wireshark Installation Complete” window, click the **Next** button



physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

☐ Click the Finish button in the “Completing Wireshark 3.6.8 64-bit Setup” window.



Uninstall any previous version of PANalyzr

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

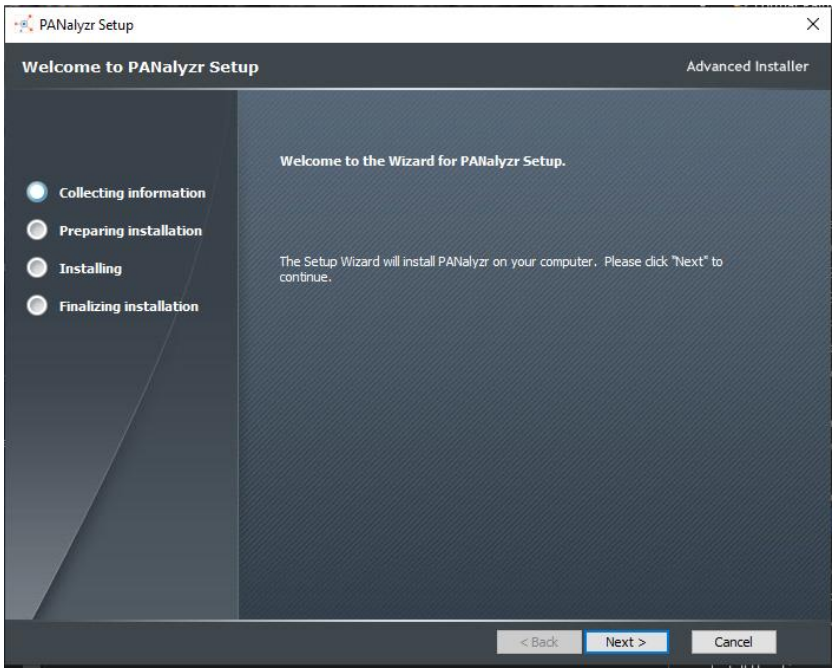
Install the PANalyzr Software

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

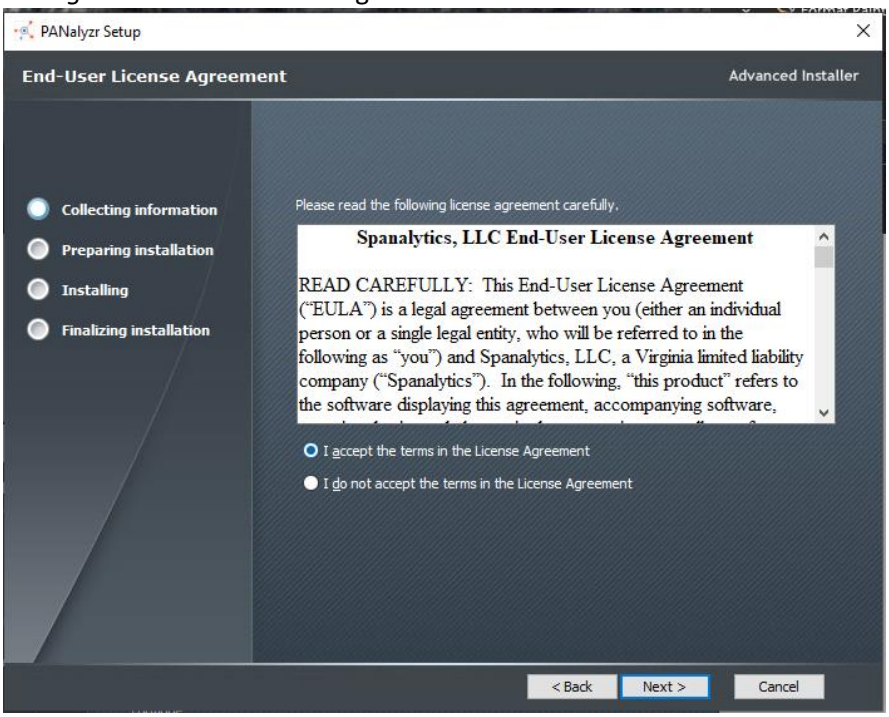
☐ Download the file **PANalyzr_Setup.exe** to the desired location on the local machine
☐ Double-click the **PANalyzr_Setup.exe** to initiate the installation process

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

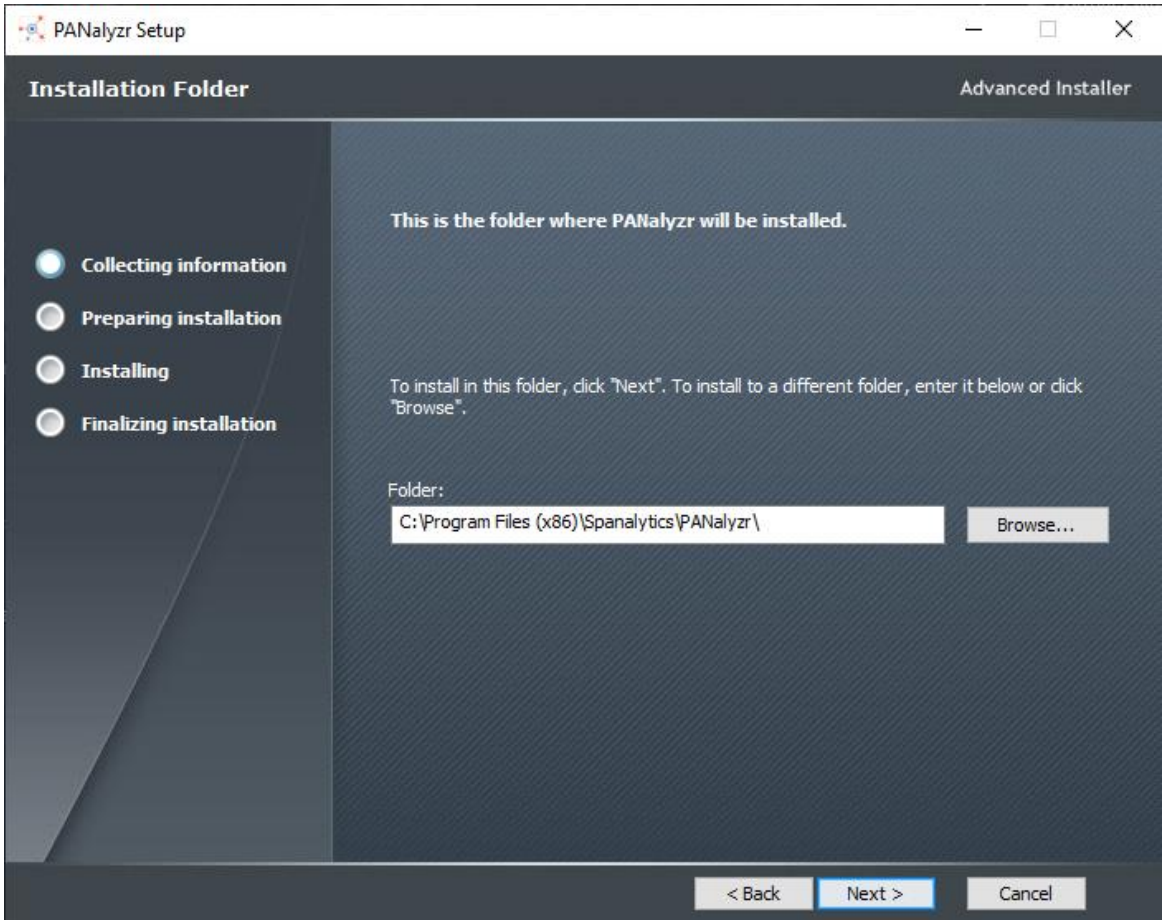


☐ The "*Spanaytics, LLC End-User License Agreement*" will be displayed in a scroll box on the *PANalyzr Installshield Wizard* window. Scroll through the "*Spanaytics, LLC End-User License Agreement*" to view the agreement documentation.



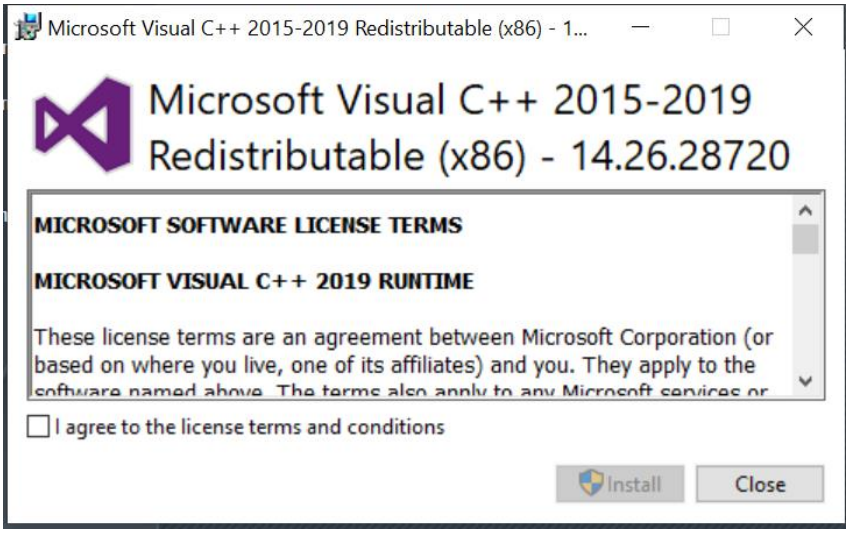
physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

- ☐ 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



physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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



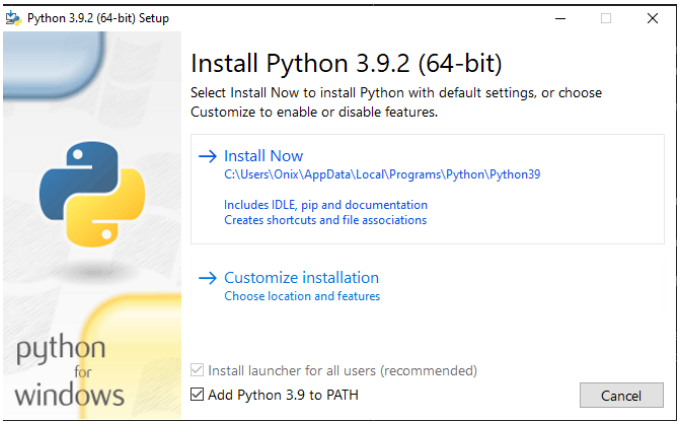
- ☐ A 'User Account Control' popup window may be displayed during the installation, prompting the user to allow the app to make changes to the device. Click the **Yes** button to continue

Install Python

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

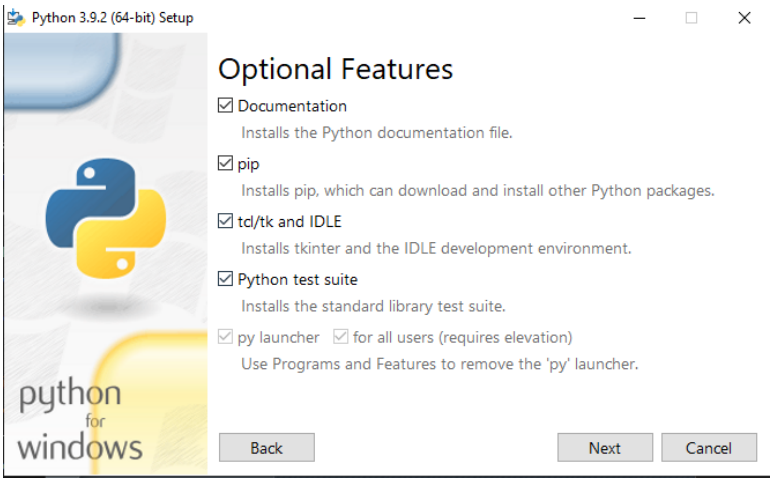
Note: Additional hardware (included with the optionally purchased PANalyzr IoT Expansion Pack hardware set) is required for Z-Wave packet capturing

- ☐ 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



physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

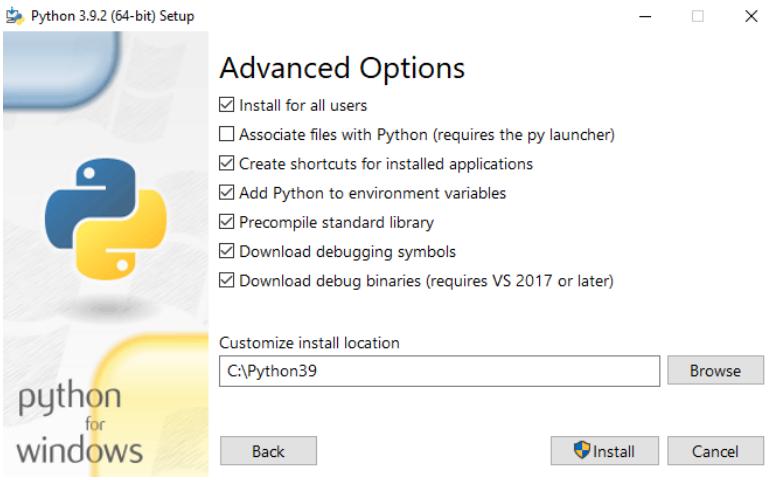
☐ In the “Optional Features” window, select the “Python test suite” box and click the **Next** button



☐ In the “Advanced Options” window, select the “Precompile standard library,” “Download debugging symbols,” and the “Download debug binaries..” boxes.

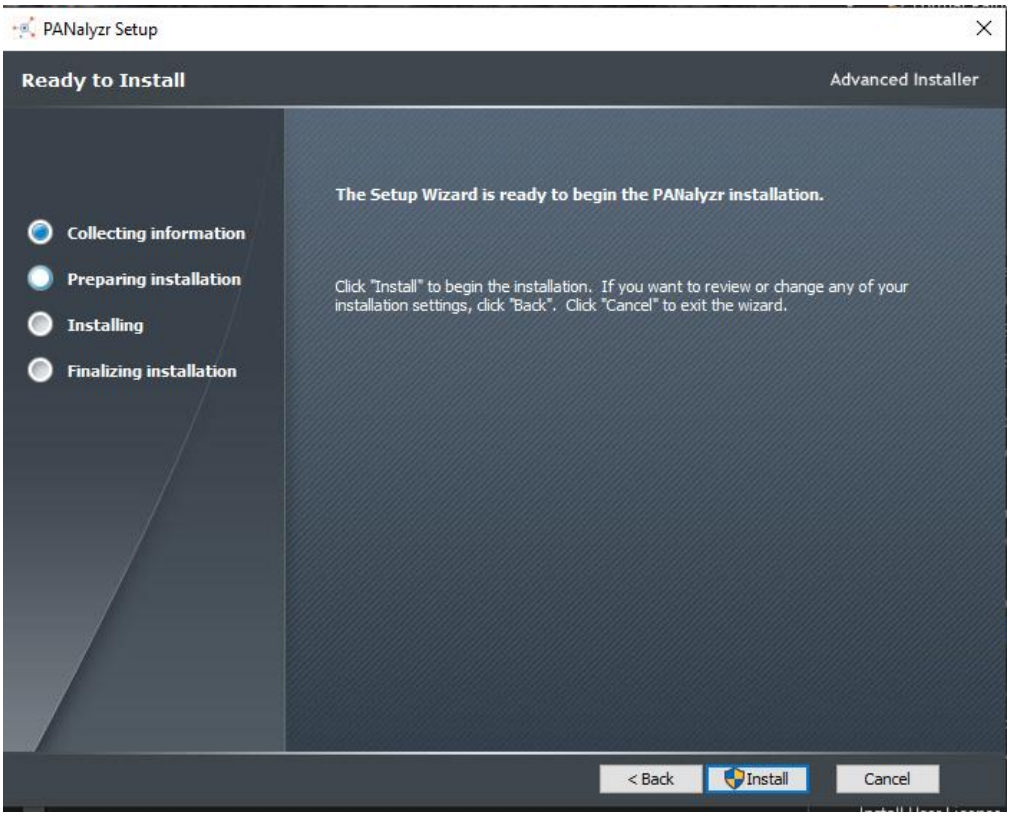
☐ Next, enter the following text in the “Customize install location” field: **C:\Python39**

☐ Click the **Install** button



physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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



Install required python package for brackle

☐ Open a Windows command prompt window

☐ Install the bitstring package by typing the following at the command prompt:
pip3 install bitstring

☐ Close the Windows command prompt window

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

Z-Wave Packet Capturing Setup

Note: Additional hardware (included with the optionally purchased PANalyzr IoT Expansion Pack hardware set) is required for Z-Wave packet capturing

Install required python package for Z-Wave packet capturing

- ☐ 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 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.

- ☐ Close all open Windows command prompt windows

Install the Z-Wave Device 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**

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 utilizing the PANalyzr protocol analyzer hardware and software.

physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com