PANalyzr™ SW Install Procedure for Windows

01/07/2022

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

v0.9.0 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

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)

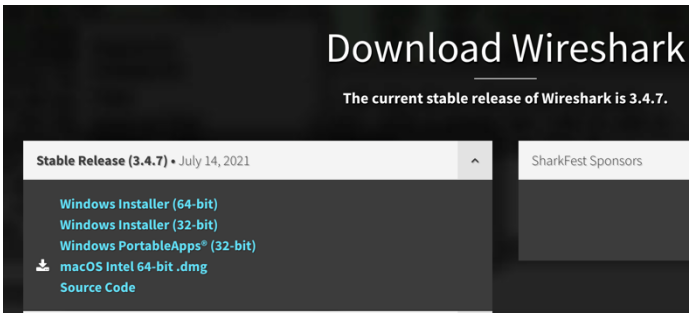
- ☐ Open a Windows File Explorer Window
- ☐ Navigate to the Wireshark Global Plugins folder (by default, this folder is usually set to ***C:\Program Files\Wireshark\plugins\3.4\epan***)
- ☐ Remove the file **panalyzr.dll** from this folder

Install Wireshark & Npcap

PANalyzr requires Wireshark version 3.6.0 (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

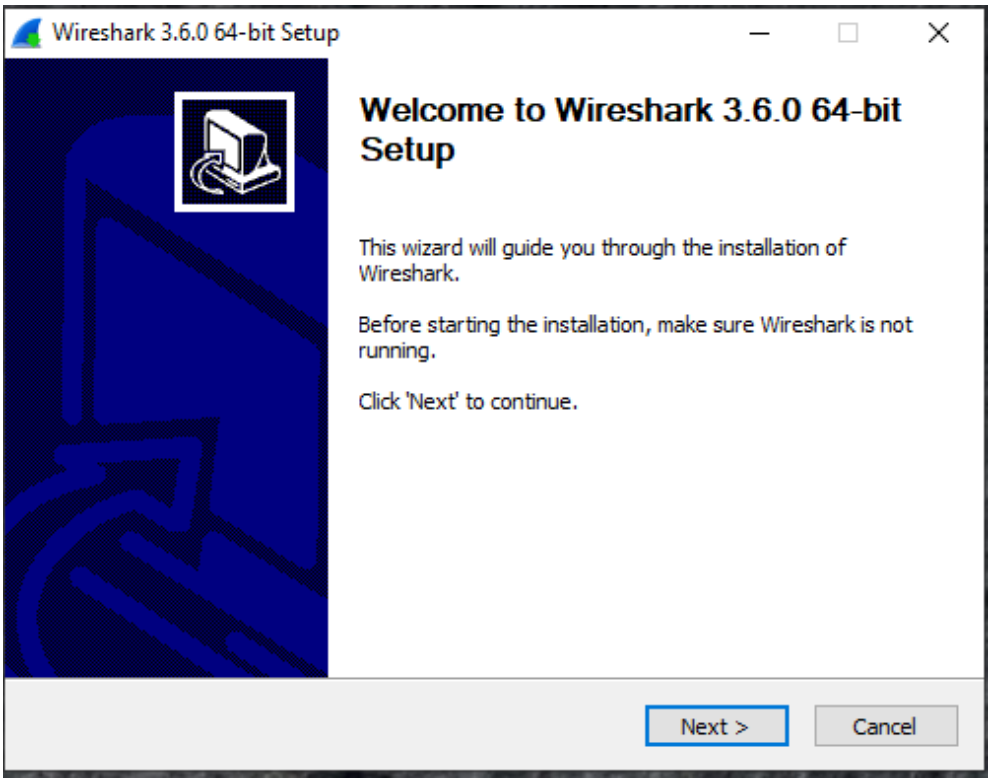
- ☐ Download the latest version of Wireshark from https://www.wireshark.org/#download



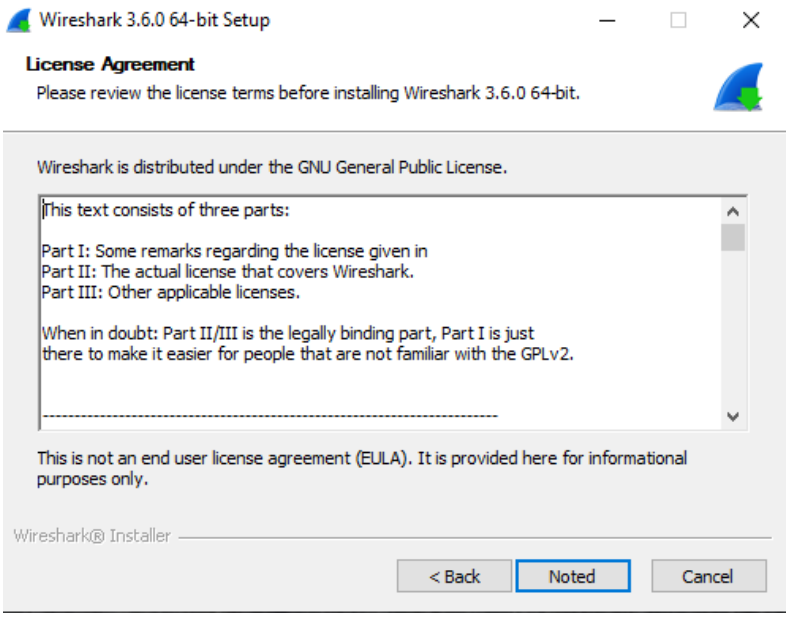
physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

☐ 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

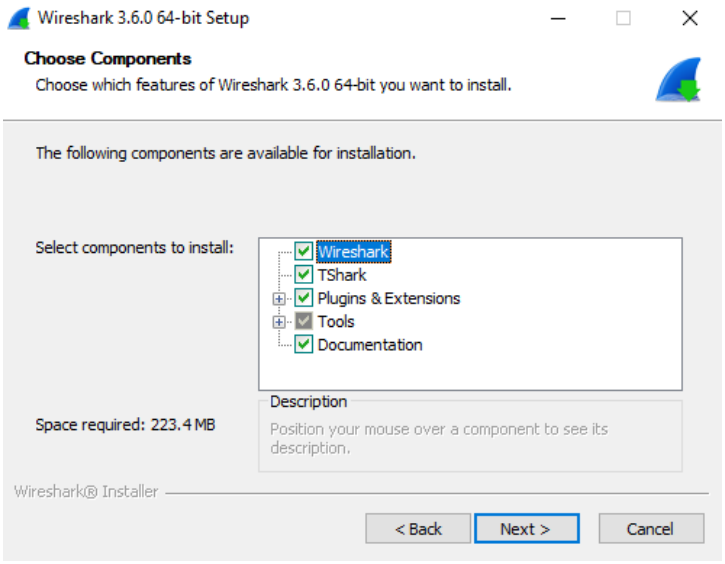


☐ In the "License Agreement" window, click on the **Noted** button

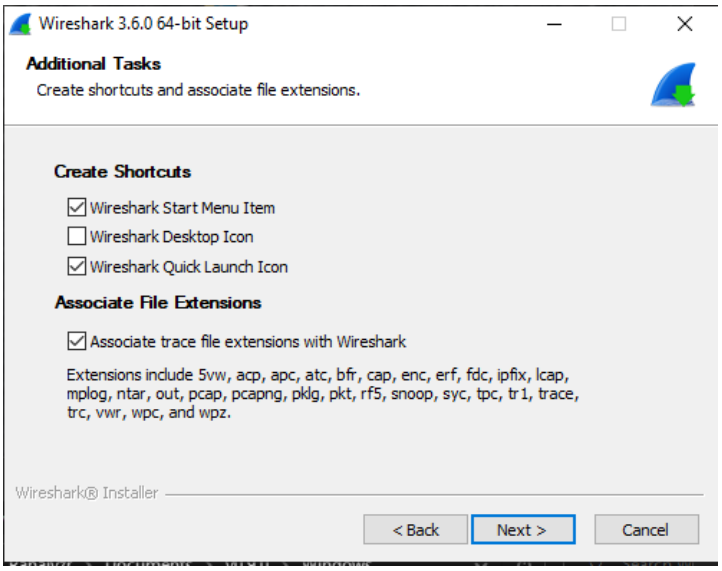


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

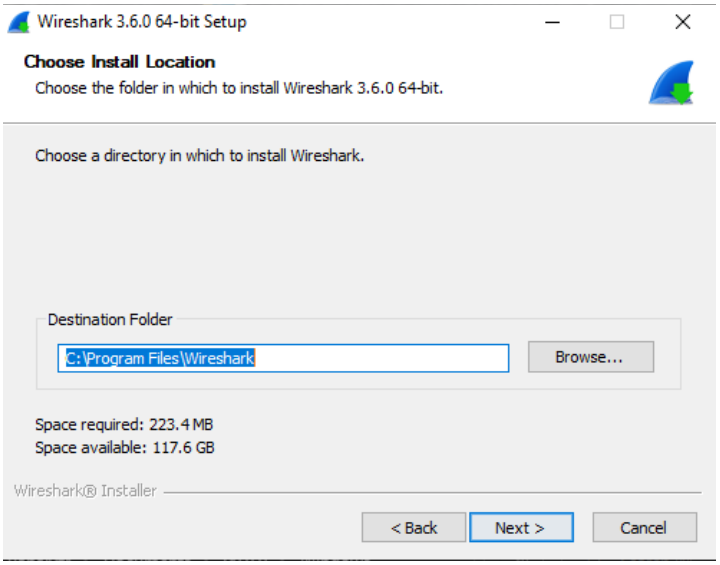


☐ In the “Additional Tasks” window, click on the **Next** button

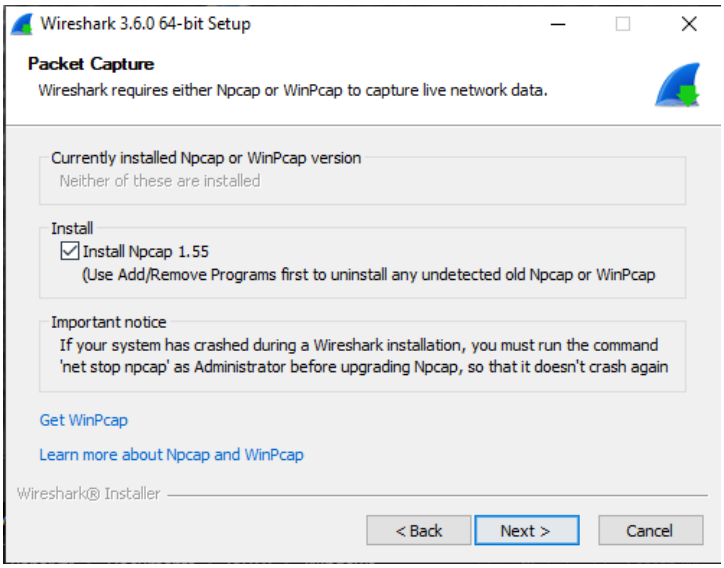


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

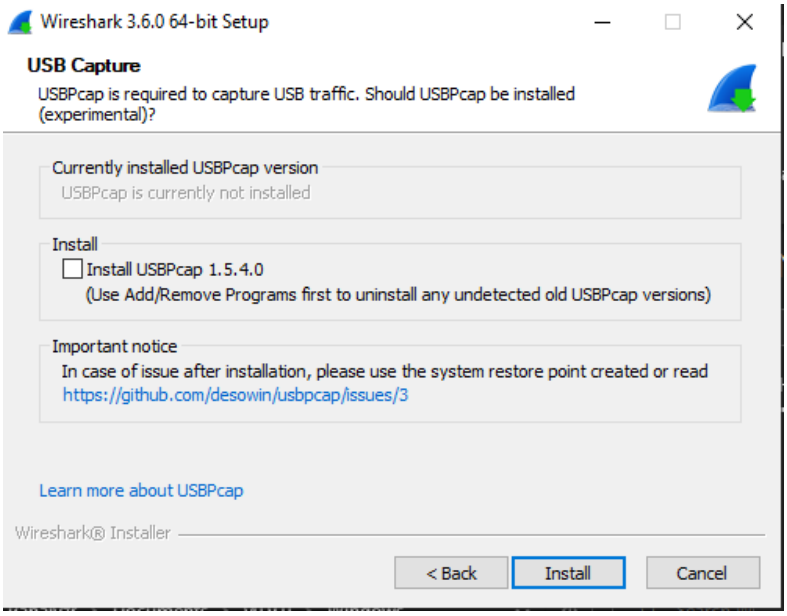


☐ In the “Packet Capture” window, select the “Install Npcap #.##” box and click on the **Next** button

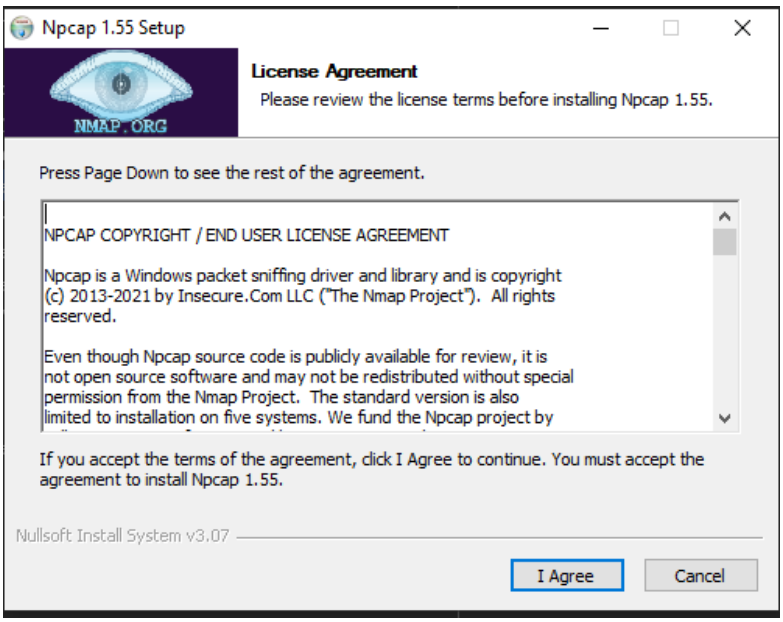


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

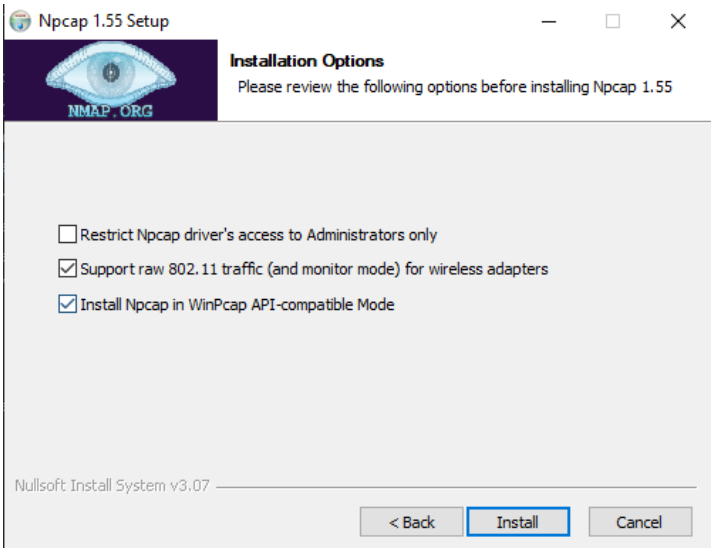


☐ In the “Npcap License Agreement” window, click the **I agree** button

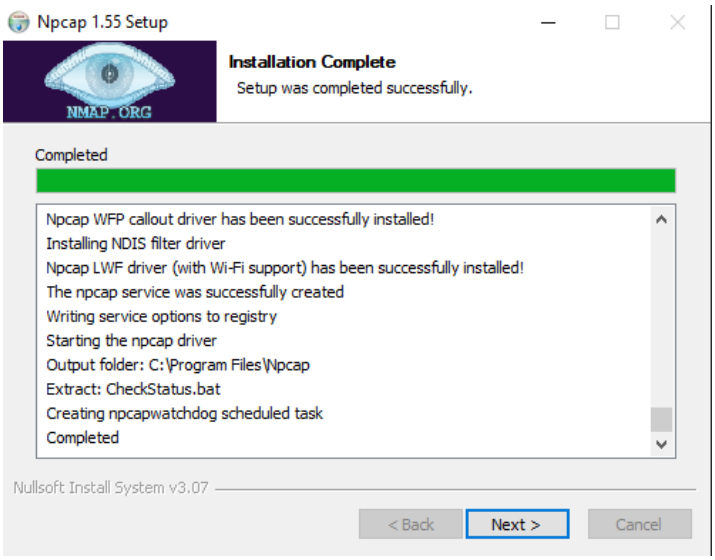


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

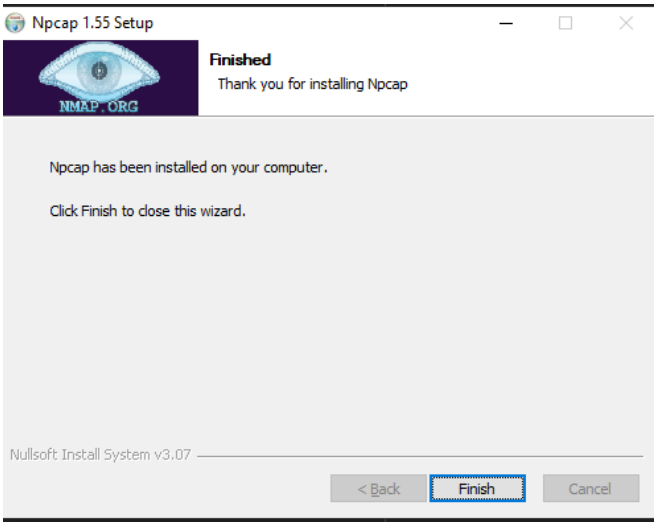


☐ In the “Installation Complete” window, click the **Next** button after the installation is complete.

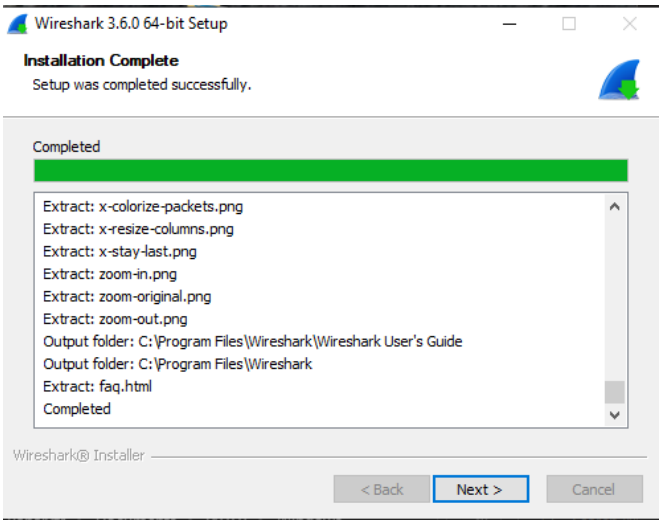


physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

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

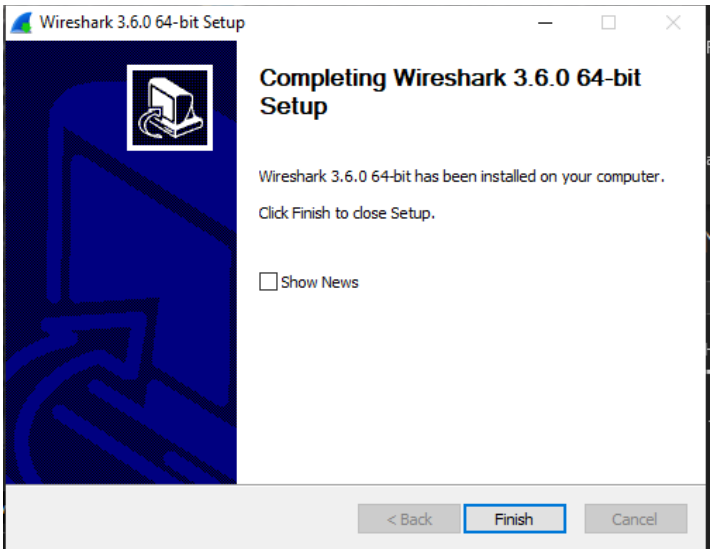


☐ In the “Wireshark Installation Complete” window, click the **Next** button



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

☐ In the “Completing Wireshark 3.4.7 64-bit Setup” window, click the **Finish** button.



Uninstall any previous version of PANalyzr

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

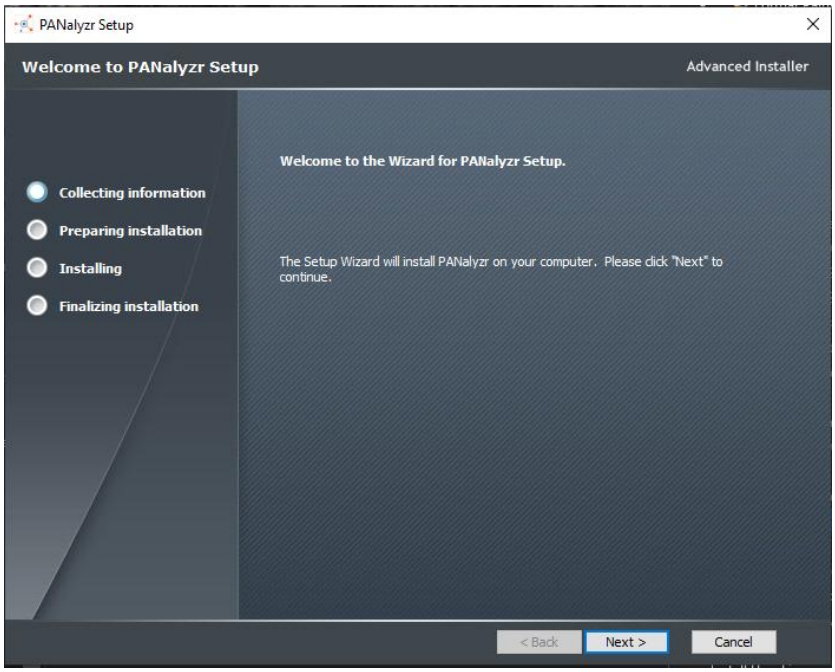
Install the PANalyzr Software

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

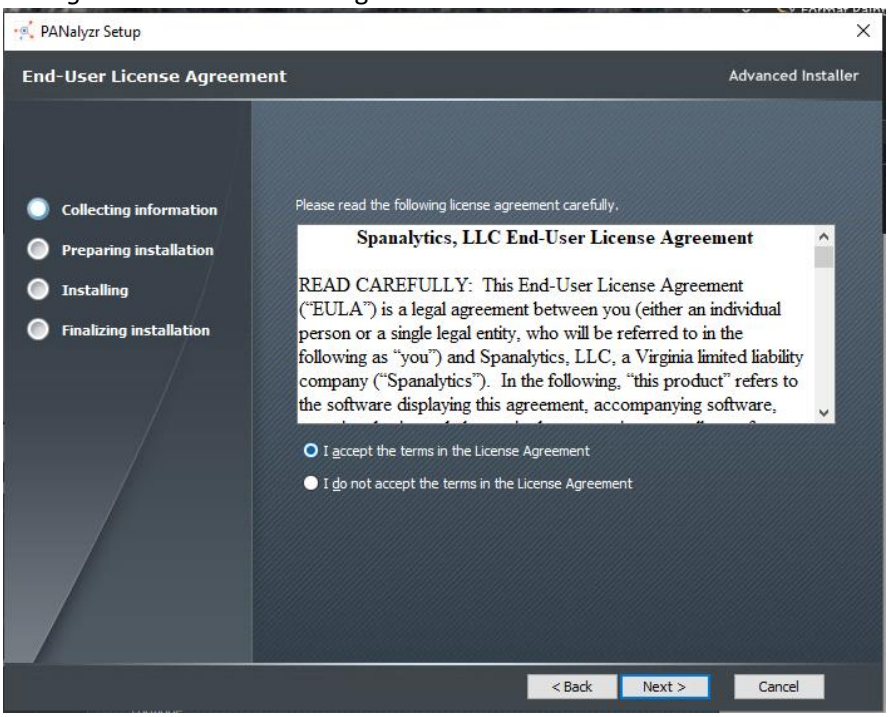
☐ Download the **PANalyzr_Setup.exe** to the desired location on the local machine
☐ Double-click the **PANalyzr_Setup.exe** to initiate the install process

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

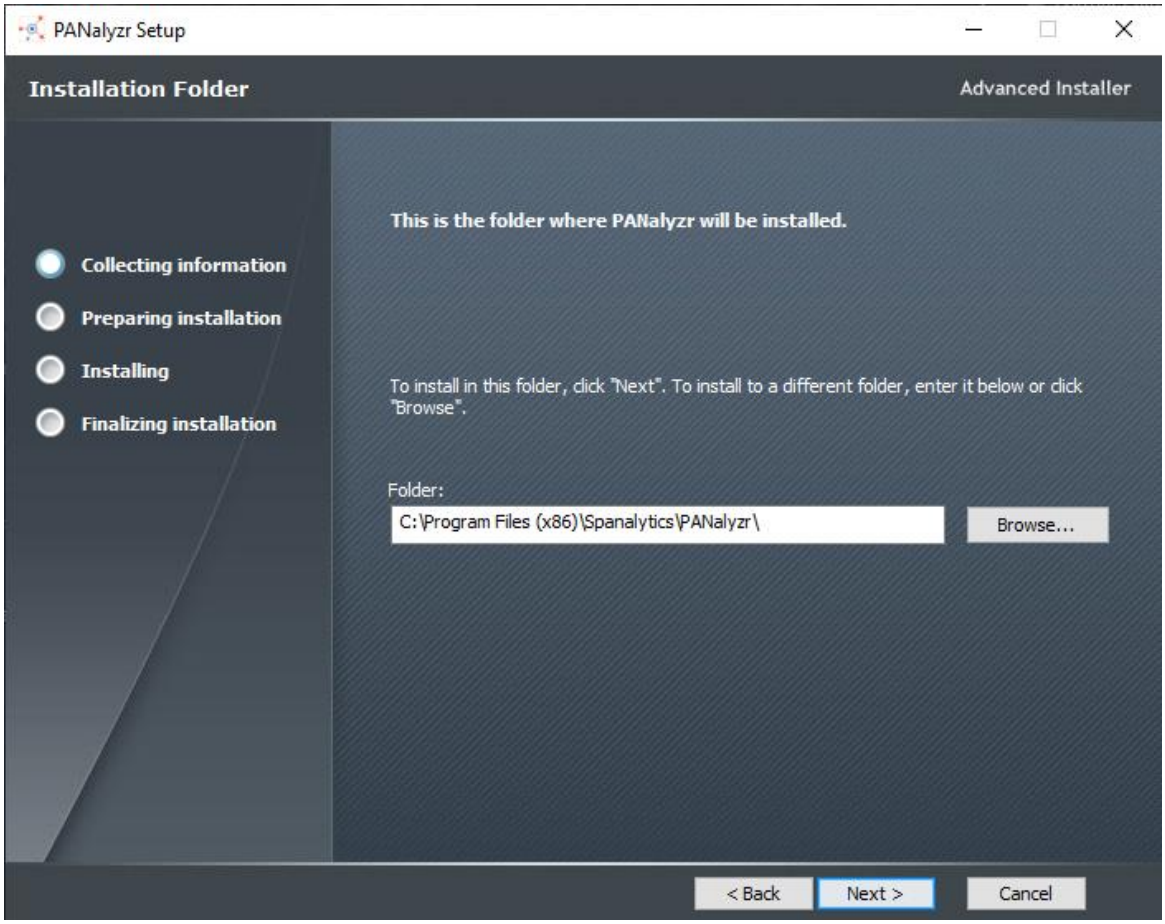


☐ The "*Spanaytics, LLC End-User License Agreement*" will be displayed in a scroll box on the *PANalyzr Installshield Wizard* window. Scroll through the "*Spanaytics, LLC End-User License Agreement*" to view the agreement documentation.



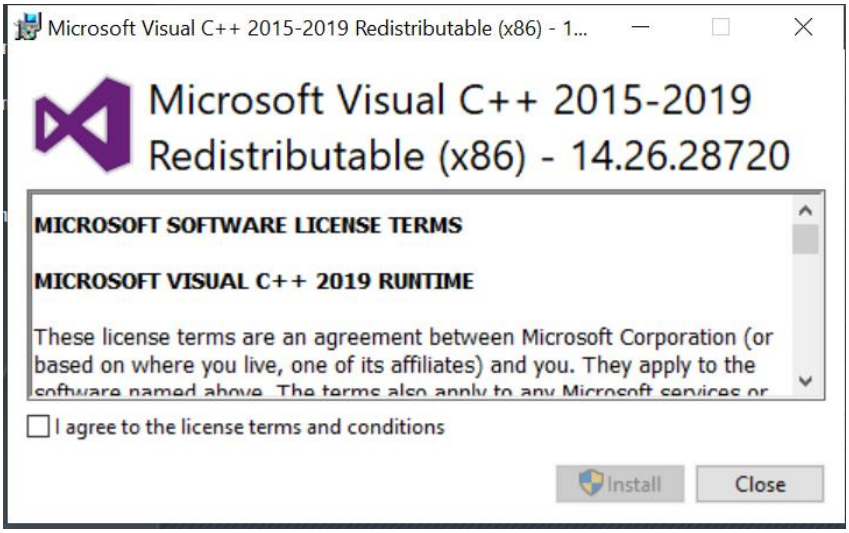
physical and mailing address: 4190 Innslake Drive, Glen Allen, VA 23060
phone: (804) 364-1050 ~ **email:** spanalytics@spanalytics.com ~ **website:** www.spanalytics.com

- ☐ 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

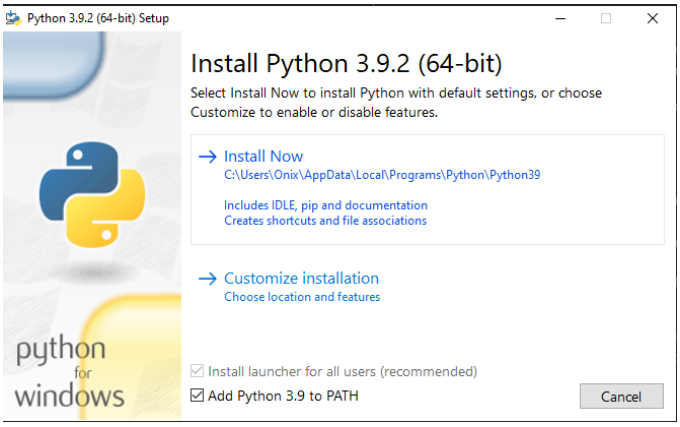


☐ During the install a popup *'User Account Control'* window may be displayed, prompting the user to allow the app to make changes to the device. Click the **Yes** button to continue

Install Python

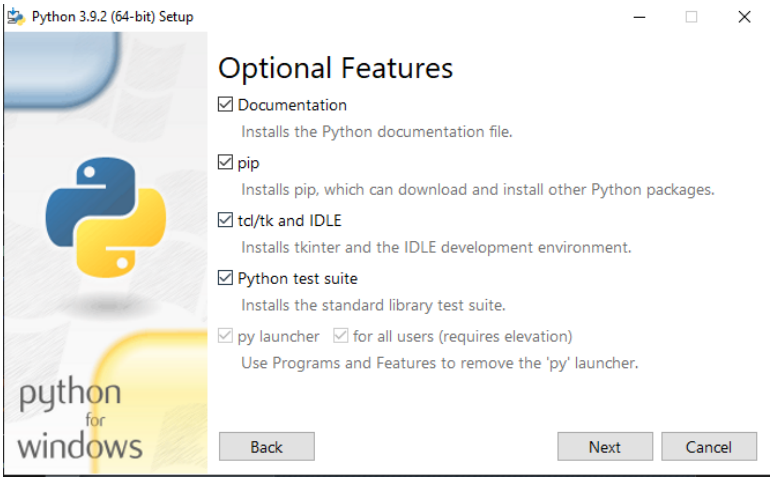
The Z-wave packet capturing and the Brackle packet decryption utilities both require Python. For both functions to work correctly, Python must be installed as described in this section.

☐ 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



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

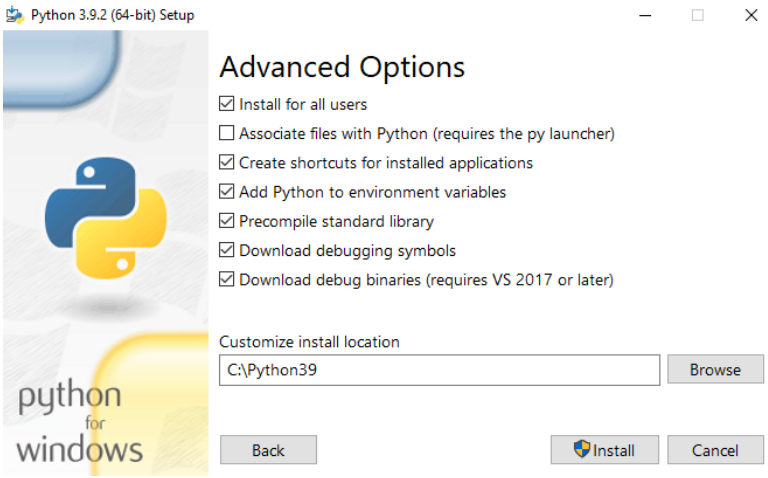
☐ In the “Optional Features” window, select the “Python test suite” box and click the **Next** button



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

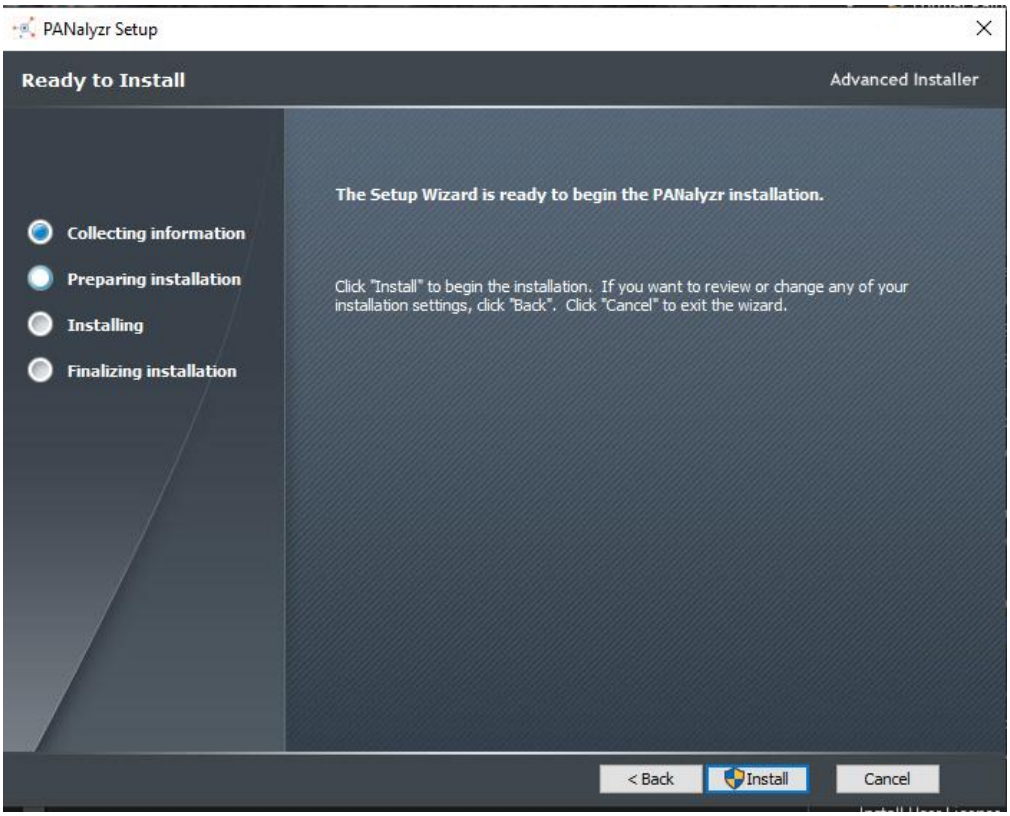
☐ Next, enter the following text in the “Customize install location” field: **C:\Python39**

☐ 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 install is complete. Click the **Finish** button to close the 'PANalyzr Wizard' 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

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.

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