

AI-01882 Zigbee 3.0 Signal Analysis Using Wireshark

Owner	© Rigel Arcayan
Tags	Project
Created time	@July 26, 2025 12:32 AM

Which Sonoff dongle to use for wire shark zigbee signal analysis? -P or -E?

For Zigbee signal analysis with Wireshark, you generally want to use a dongle that can be flashed with sniffer firmware. Both the Sonoff ZBDongle-P and ZBDongle-E can be used for this purpose, but there's a common consensus and more readily available sniffer firmware/guides for specific chipsets..

Here's a breakdown:

- Sonoff ZBDongle-P (based on TI CC2652P): This dongle is widely recommended for Zigbee sniffing. It uses the Texas Instruments CC2652P chip, and there's well-established sniffer firmware available (often from Texas Instruments themselves, like SmartRF Packet Sniffer 2 firmware). Many guides and communities, including those for Home Assistant and Zigbee2MQTT, show how to flash the ZBDongle-P for sniffer mode and use it with Wireshark. Its popularity makes it easier to find support and resources.
- Sonoff ZBDongle-E (based on EFR32MG21): The ZBDongle-E uses a Silicon Labs EFR32MG21 chip. While it can be used as a sniffer, it might require different firmware and tools compared to the TI-based P version. Some users have reported it being a bit less "cooked" in terms of readily available sniffer firmware and community support specifically for sniffing compared to the -P model. However, there are resources and custom firmware available if you're comfortable with that.

Recommendation:

For general ease of use and readily available resources for Zigbee signal analysis with Wireshark, the Sonoff ZBDongle-P is generally the preferred choice. It has a more mature ecosystem for sniffer firmware and integration

with Wireshark.

Key steps involved in using either dongle as a sniffer:

- Flash Sniffer Firmware: You'll need to reflash the dongle with specific sniffer firmware. This will overwrite its default coordinator/router firmware.
- Install Wireshark: Make sure you have Wireshark installed on your computer.
- Install Necessary Drivers/Extcaps: Depending on the dongle and your operating system, you might need specific drivers or Wireshark "extcaps" (external capture plugins) to properly interpret the data from the dongle.
- Configure Wireshark: You'll need to configure Wireshark to listen on the correct interface/pipe and potentially add Zigbee decryption keys (like the Trust Center Link Key and Network Key) to see meaningful data.

No matter which dongle you choose, be aware that reflashing it for sniffing will make it unable to function as a Zigbee coordinator or router without reflashing it back to its original firmware.

Copilot version

To analyze Zigbee signals in Wireshark, the best choice is the SONOFF Zigbee 3.0 USB Dongle Plus-E. Here's why it stands out:

Why the Plus-E Model Works for Sniffing

- It supports 802.15.4 packet capture, which is the low-level protocol Zigbee is built on.
 - You can flash it with sniffer firmware that converts Zigbee traffic into a format Wireshark can understand A.
 - Once flashed, it sends packets in JSON format over USB serial, which Wireshark can interpret using an Extcap plugin A.

Important Notes

- Flashing the sniffer firmware replaces the coordinator firmware, so the dongle can no longer be used for Zigbee2MQTT or Home Assistant until you reflash it back A.
 - You'll need to install the Extcap plugin for Wireshark to decode the packets properly. This is available in the GitHub repository for the sniffer firmware.

Setup Essentials

- SONOFF Zigbee 3.0 USB Dongle Plus-E
 - Windows 10 or 11 PC
 - Wireshark installed
 - Sniffer firmware and Extcap plugin from GitHub

If you're using the Plus-P model (CC2652P), it's not officially supported for sniffing due to differences in RF libraries B—so stick with the Plus-E for reliable results.

Want help flashing the firmware or setting up Wireshark filters? I can walk you through it step by step.

Absolutely, Rigel—let's transform that SONOFF Plus-E into a Zigbee sniffer for Wireshark. Here's a step-by-step guide:

What You'll Need

- SONOFF Zigbee 3.0 USB Dongle Plus-E (EFR32MG21)
 - Windows PC
 - USB extension cable (recommended to reduce RF interference)
 - EFR32 sniffer firmware
 - EFR32 Command Line Interface Tool (efr32cli) or Silicon Labs' Simplicity Commander
 - Wireshark with Extcap plugin from the same GitHub repo

Step-by-Step Flashing Instructions

1. Install the Flashing Tool

You can use Simplicity Commander:

- Download from Silicon Labs: Simplicity Studio
 - After installation, locate the tool `commander.exe`

1. Download the Sniffer Firmware

- Go to GitHub releases
 - Download the latest `.hex` firmware file (e.g., `sniffer-usb.hex`)

1. Put the Dongle in Bootloader Mode

- Hold the BOOT button, then plug the dongle into USB
 - Release the BOOT button once powered

1. Flash the Firmware

Using Simplicity Commander:

```
commander.exe flash --device EFR32MG21 --firmware sniffer-usb.hex
```

✓ If successful, you'll see a confirmation message like "Programming Successful."

1. Verify Connection

After flashing, the dongle should show up as a COM port. You can use a serial monitor (like PuTTY) to verify it outputs Zigbee frames in JSON format.

Capturing Zigbee in Wireshark

1. Install Wireshark

- Download from [wireshark.org](https://www.wireshark.org)

1. Install Extcap Plugin

- Get it from the same GitHub repo and place it in Wireshark's `extcap` directory.

1. Configure Sniffing

- Launch Wireshark → Capture → Options → Choose the Extcap interface for Zigbee
 - Start capture and observe Zigbee traffic in real time!

Let me know if you want help setting filters or decoding specific frames—or if you'd like to flash it back later for coordinator use. You're doing some solid radio work here! 📡

Alternate Method

Using a Sonoff ZBDongle-E with Wireshark involves two key stages: flashing the dongle with the correct sniffer firmware and then configuring Wireshark to capture and decrypt the Zigbee traffic.

Flashing the Firmware

The ZBDongle-E comes pre-flashed with Zigbee coordinator firmware, so you must replace it with sniffer firmware to use it with Wireshark. The process can be done easily with the official SONOFF Dongle Flasher web tool.

1. **Identify your dongle:** The ZBDongle-E uses an EFR32MG21 chip, which is different from the ZBDongle-P. Ensure you are using the correct firmware for your model.
 2. **Access the flashing tool:** Navigate to the official SONOFF Dongle Quick Flasher web tool at <https://dongle.sonoff.tech/sonoff-dongle-flasher/>.
 3. **Connect the dongle:** Plug the ZBDongle-E into a USB port on your computer and click the '**Connect**' button on the web page. You may need to confirm the connection twice.
 4. **Select sniffer firmware:** From the list of available firmwares, select the sniffer firmware for the ZBDongle-E. This firmware will enable the device to capture 802.15.4 packets (the protocol Zigbee is based on).
 5. **Flash the firmware:** Click '**Flash**' to begin the process. The tool will download and install the new firmware on your dongle. This should only take about a minute.
-

Configuring Wireshark for Capture

Once the dongle has the sniffer firmware, you can set up Wireshark to capture and analyze the Zigbee traffic.

1. **Install Wireshark:** Download and install the latest version of Wireshark. Make sure to install Npcap if you are on Windows.
2. **Install the Wireshark Extcap:** The flashed dongle sends captured packets in a specific format (JSON over a serial port). Wireshark needs an **Extcap** (External Capture) plugin to correctly interpret this data. Some sniffer firmware repositories provide this `.exe` file. You need to copy this file into the correct Wireshark `extcap` folder. To find the folder location, go to [Help > About Wireshark](#) and select the `Folders` tab.
3. **Start capturing:** Plug the ZBDongle-E into a USB port. Open Wireshark. You should see a list of available COM ports at the bottom of the main window. Look for the one that corresponds to your dongle.
4. **Configure capture settings:** Click the gear icon next to your dongle's COM port in Wireshark. This will bring up a configuration window. Here, you can

select the Zigbee channel you want to sniff. The channel must match the one used by your Zigbee network.

5. **Add decryption keys:** To view the contents of the Zigbee packets (which are encrypted), you must add the network's encryption keys to Wireshark.

- Go to `Edit > Preferences > Protocols > Zigbee` .
- Set the **Security Level** to `AES-128 Encryption, 32-bit Integrity Protection` .
- Click the `Edit` button next to `Pre-configured keys` .
- Add the **Trust Center link key**, which is a standard key for most Zigbee networks: `5A:69:67:42:65:65:41:6C:6C:69:61:6E:63:65:30:39` .
- Add your network's **Transport Key**. This key is unique to your network. You can often find it in the configuration files of your Zigbee gateway (like Zigbee2MQTT). You may need to convert it to a colon-separated hex format. Alternatively, if a new device joins the network while you are sniffing, Wireshark will capture an unencrypted "Transport Key" message that you can use.

6. **Start the capture:** Once the keys are added, you can start the capture. Wireshark will now display all the Zigbee traffic on the selected channel, with the ability to decrypt the messages you have the keys for.

A step-by-step video on flashing the Sonoff Zigbee Dongle-E is available here: [Upgrade Your Sonoff Zigbee Dongle-E with Confidence in Minutes](#). This video provides a visual guide on the process of updating the dongle's firmware.

I'm running the Zigbee capture and there are a lot of data scrolling. Train me on how to use it to analyze my Zigbee network and device.

Analyzing the Zigbee traffic in Wireshark requires you to filter the raw data, understand the packet types, and follow the communication flow between devices.

Step 1: Filter the Noise

The first step is to clean up your view so you're only seeing Zigbee-related traffic. The packets from your sniffer are often encapsulated in other protocols like UDP.

- **Display Filter:** Use the display filter bar at the top of the Wireshark window.

- To see only Zigbee packets, use the filter `zbee`.
 - To see the underlying protocol used by your sniffer dongle (often Zigbee Encapsulation Protocol or **ZEP**), you might need to use `zep` or a more specific filter like `udp.port == 17754 && !icmp` to exclude other network noise.
 - **Apply the `zbee` filter:** Once you have the correct network and trust keys configured, this filter will be your primary tool for analysis.
-

Step 2: Understand the Packet Breakdown

Wireshark presents the data in a three-pane view.

- **Top Pane (Packet List):** This is a summary of each packet. Columns like **Source**, **Destination**, **Protocol**, and **Info** are crucial.
 - **Source/Destination:** These will be the short addresses (16-bit) of the Zigbee devices. These are assigned dynamically and can be changed. You can map these to the device's unique **Extended PAN ID** (64-bit address) for easier identification.
 - **Info:** This field provides a high-level summary of the packet content, such as "Device Announcement," "ZCL Read Attributes," or "ZCL Report Attributes."
 - **Middle Pane (Packet Details):** This pane shows the protocol stack of the selected packet. You'll see layers like `IEEE 802.15.4` (the physical and MAC layers), `Zigbee Network Layer`, `Zigbee Application Support Layer`, and finally, the `Zigbee Cluster Library (ZCL)`.
 - **ZCL:** This is where the real application data is. Expand this layer to see the command being sent, such as a smart light turning on/off or a sensor reporting temperature.
 - **Bottom Pane (Hex Dump):** This shows the raw data of the packet in hexadecimal format. It's useful for advanced debugging but can usually be ignored for basic analysis.
-

Step 3: Analyze Common Communication Flows

- **Device Joining the Network:** When a new device joins, you'll see a series of packets. Look for an unencrypted **Transport Key** message from the coordinator to the joining device. This is the packet you can grab the network key from if you haven't already.
- **Device Announcements:** A `Device Announcement` packet is sent by a device after it joins the network or reboots. It announces its presence and capabilities to the rest of the network. This is useful for identifying new or restarted devices.
- **Reporting Attributes:** This is the most common type of packet you'll see from sensors. A `ZCL Report Attributes` message contains the sensor's data, like a motion sensor reporting a `0` or `1` for motion or a temperature sensor reporting a value.
- **Command Packets:** These are packets sent to a device to control it. For example, a `ZCL Read Attributes` command is used to request the current state of a device, while a `ZCL Write Attributes` command can be used to set a value, like dimming a light.
- **Following the Conversation:** To track a specific interaction, right-click on a packet in the top pane and select **"Follow" > "Zigbee Stream."** This will filter the display to show only the packets exchanged between those two devices, making it much easier to analyze the complete conversation.

Tip: Map Device Addresses

Zigbee devices use short addresses that can change. To make sense of your capture, it's a good practice to create a lookup table.

1. Find a `Device Announcement` packet for each device.
2. Note the 64-bit **Extended PAN ID** (the device's unique MAC address) and its corresponding 16-bit **short address**.
3. As you analyze the capture, you can use these IDs to easily identify which device is which.