Lab 2: Decrypt Z-Wave RF Frames using the Zniffer

This hands-on exercise will demonstrate how to decrypt Z-Wave RF frames using the Z-Wave Zniffer tool.

This exercise is part of the series “Z-Wave 1-Day Course”.

1: Include using SmartStart

2: Decrypt Z-Wave RF Frames using the Zniffer

3A: Compile Switch On/Off and Enable Debug

3B: Modify Switch On/Off

4: Understand FLiRS devices

KEY FEATURES

- Decrypt Z-Wave RF Frames
- Learn to use Z-Wave Zniffer tool
- Introduction to Z-Wave Command Classes.

1 Introduction

In this exercise, we will use the Z-Wave Zniffer tool to decrypt the RF traffic when knowing the security keys for the network.

We will decrypt Z-Wave frames and get a basic understand of the Z-Wave Command Classes.

1.1 Hardware Requirements

- 1 WSTK Main Development Board
- 1 Z-Wave Radio Development Board: ZGM130S SiP Module
- 1 UZB Controller
- 1 USB Zniffer

1.2 Software Requirements

- Simplicity Studio v4
- Z-Wave 7 SDK
- Z-Wave PC Controller
- Z-Wave Zniffer

Figure 1: Main Development Board with Z-Wave SiP module

1.3 Prerequisites

You need to have setup a Z-Wave network with a Controller and a Switch On/Off slave device.

For instructions in how to setup the network, refer to the previous exercise “1 Include using SmartStart”.

2 Capture RF Packages using the Zniffer

In the previous exercise “1 Include using SmartStart”, we learned how to include a device using SmartStart and we tested the basic functionality using the PC Controller.

2.1 Setup Zniffer

Now, let’s use the Zniffer to see which frames are being sent to turn on and off the LED.

1. Make sure your Zniffer is plugged into your PC and open the Z-Wave Zniffer tool from Simplicity Studio Tools menu.
2. Select the COM port by clicking on the icon next to Port. This will search for connected Zniffers.
3. Select the COM port in the drop down menu.
4. Select the Frequency by clicking on the icon next to Frequency.
5. Select the Frequency that matches the frequency you programmed your device with. These exercises uses “EU”.
6. Start a new Trace .

The Zniffer tool is now ready and listening for Z-Wave RF Traffic.

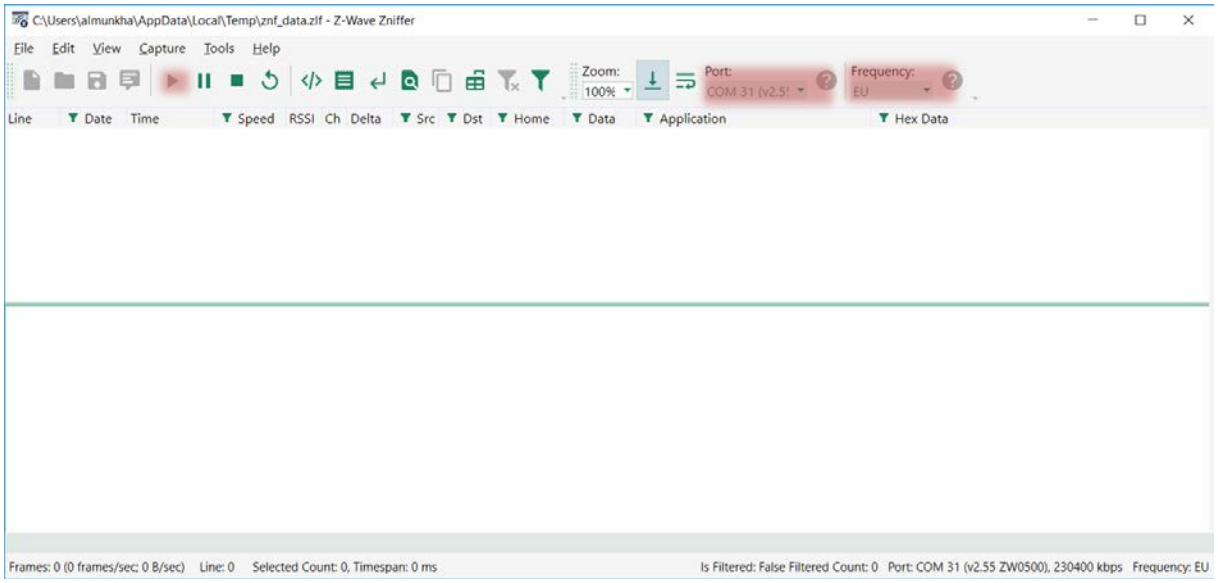

Figure 2: Zniffer Setup and Listening for Z-Wave Traffic

You might see other traffic, despite you are not sending any to your device. Currently, the Zniffer is configured for listening for any traffic in the selected region. We need to filter the trace by “Home ID” to only show traffic from your network.

1. From the PC Controller, find the “Home ID” in the “Network Management” tab.
   a. In Figure 3, the example HomeID is E2 16 BB FE.
2. Knowing the Home ID, click the small icon next to “Home” in the Zniffer. Refer to Figure 4.
3. Write the Home ID in this field and click OK.
4. The green icon now turns red symbolizing the Zniffer is filtering on Home Id.

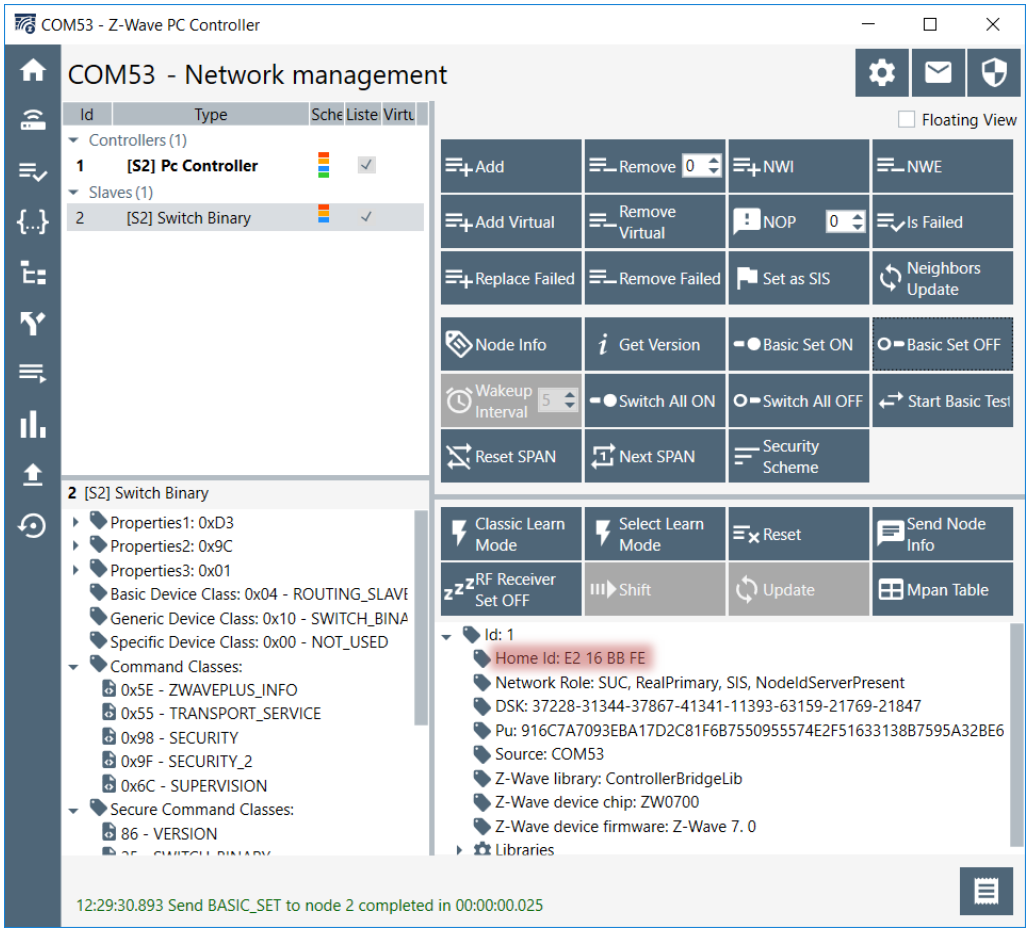

Figure 3: Home ID from PC Controller

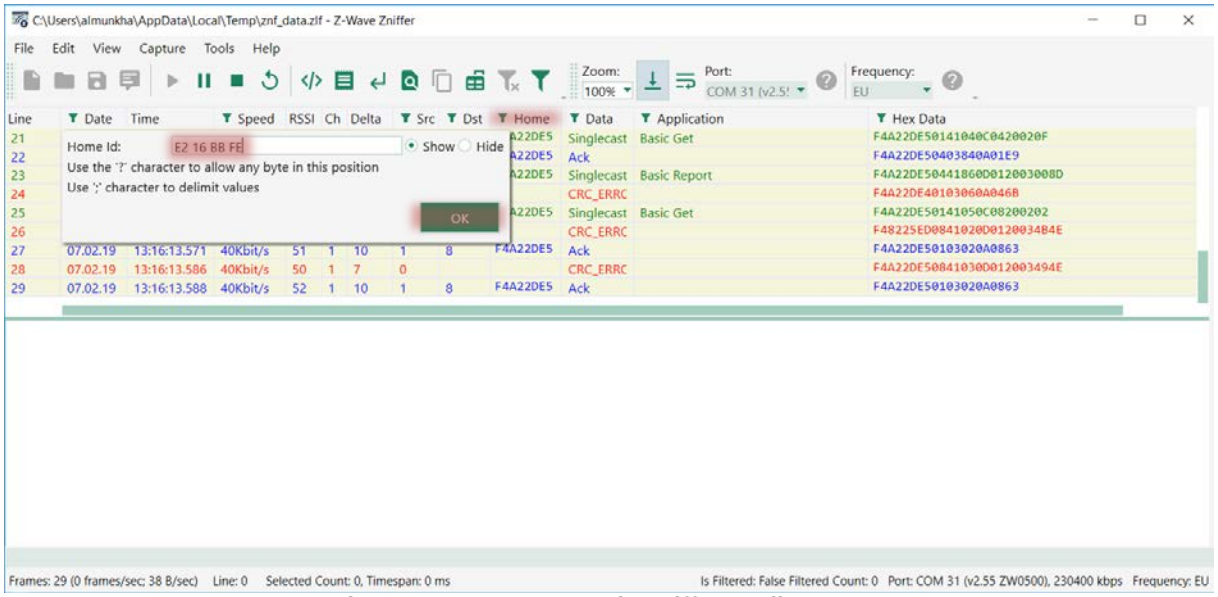

Figure 4: Insert Home ID in Zniffer to Filter Trace

Hint If you press on "Enter" on the keyboard, instead of clicking OK in the pop-up box, the filter is not applied. This means, the symbol will not turn red. Turn on the filter by clicking on Toggle Filter  in the menu bar.

2.2 Update Zniffer Nonce and SPAN Table

Nonce is only exchanged once during inclusion and is used to calculate subsequent SPANs in order to prevent replay attacks.

SPAN becomes out of sync if the message did not reach the destination. A new Nonce must then be requested to update the SPAN table.

As such; In order to decrypt a Z-Wave RF frame you need two things:

- The security keys for the network
- The Nonce key/SPAN table

This section will introduce how to add this information to the Zniffer so it can decrypt the individual frames.

> ***Hint:*** More information on the key exchange can be found the Knowledge Base:
>
> Secure S2 key exchange methods during inclusion

If a trace was started during inclusion, the trace will already contain the Nonce key and thus be able to calculate the SPANs. However, in this exercise we have not the inclusion process in our Zniffer trace and therefore we must provide the Nonce key to the Zniffer.

1. Make sure the Zniffer is still tracing as instructed in section 2.1.
2. In the PC Controller, click on Reset SPAN.
3. In the PC Controller, click on Basic Set ON. This will send a command to the device, which then triggers a reset of SPAN.
4. In the PC Controller, click on Basic Set OFF to turn off the LED again.

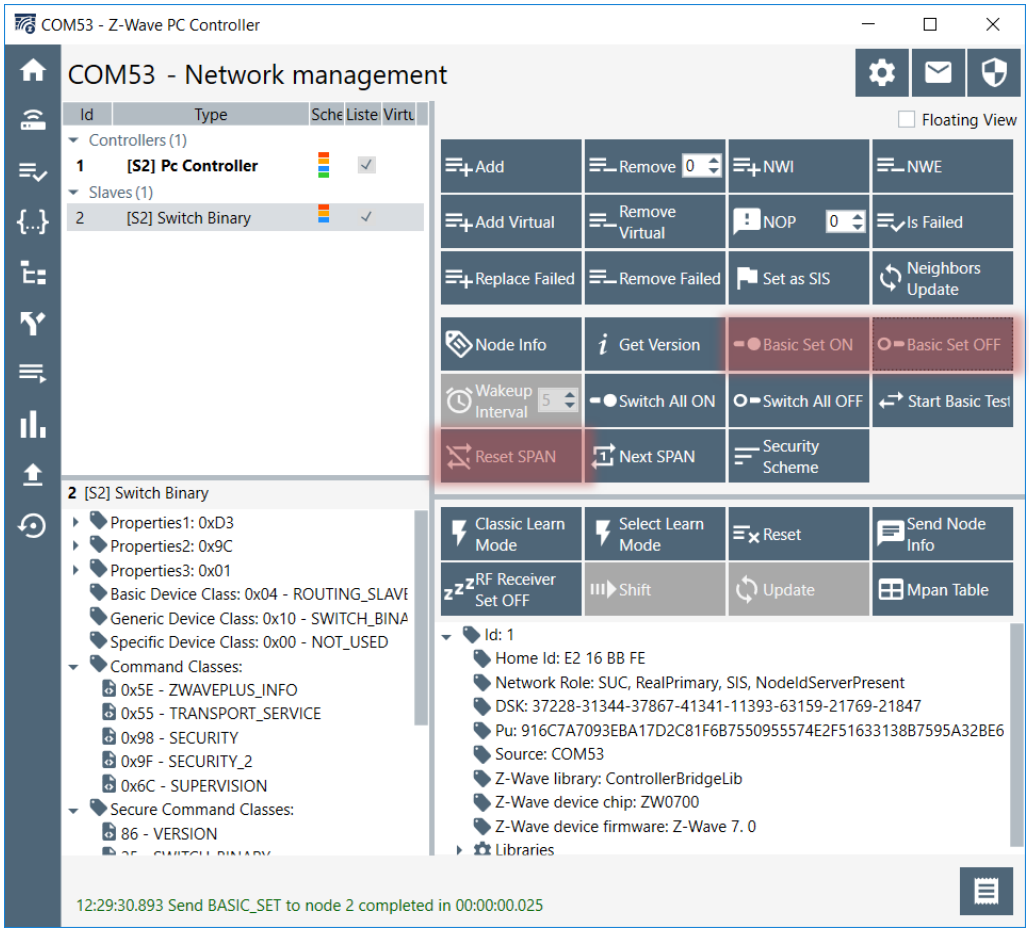

Figure 5: Reset SPAN in PC Controller

Return to the Zniffer tool and notice the following:

- A “Nonce Get” and a response “Nonce Report’ is shown.
- Some encrypted S2 Messages that we cannot yet decrypt.

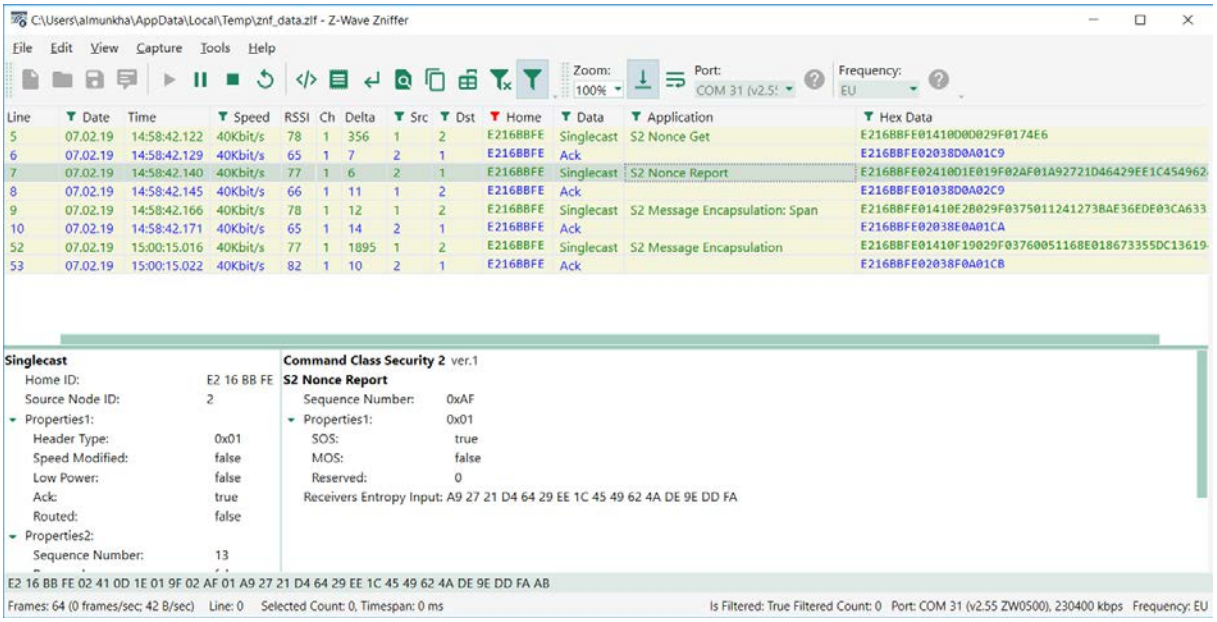

Figure 6: SPAN Reset and Encrypted S2 messages

The frames we see in the Zniffer are still encrypted. We are still missing the network keys. Return to the PC Controller to find the needed network key.

- You can find the keys in the PC Controller by clicking on the icon  in the upper right corner.
- Network keys for all security groups are shown in the pop-up window, refer to Figure 7.
  - S0
  - S2 Unauthenticated
  - S2 Authenticated
  - S2 Access
- Since our device is included as S2 Authenticated using the DSK, we will be needed in S2 Authenticated key.
  - In Figure 7, the example key is: D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3
- Click on the “Copy to Clipboard”  .

Hint: More information on the security groups can be found the Knowledge Bases:

Is S2-AccessControl more secure than S2-Authenticated?

Why use S2-Unauthentucated?

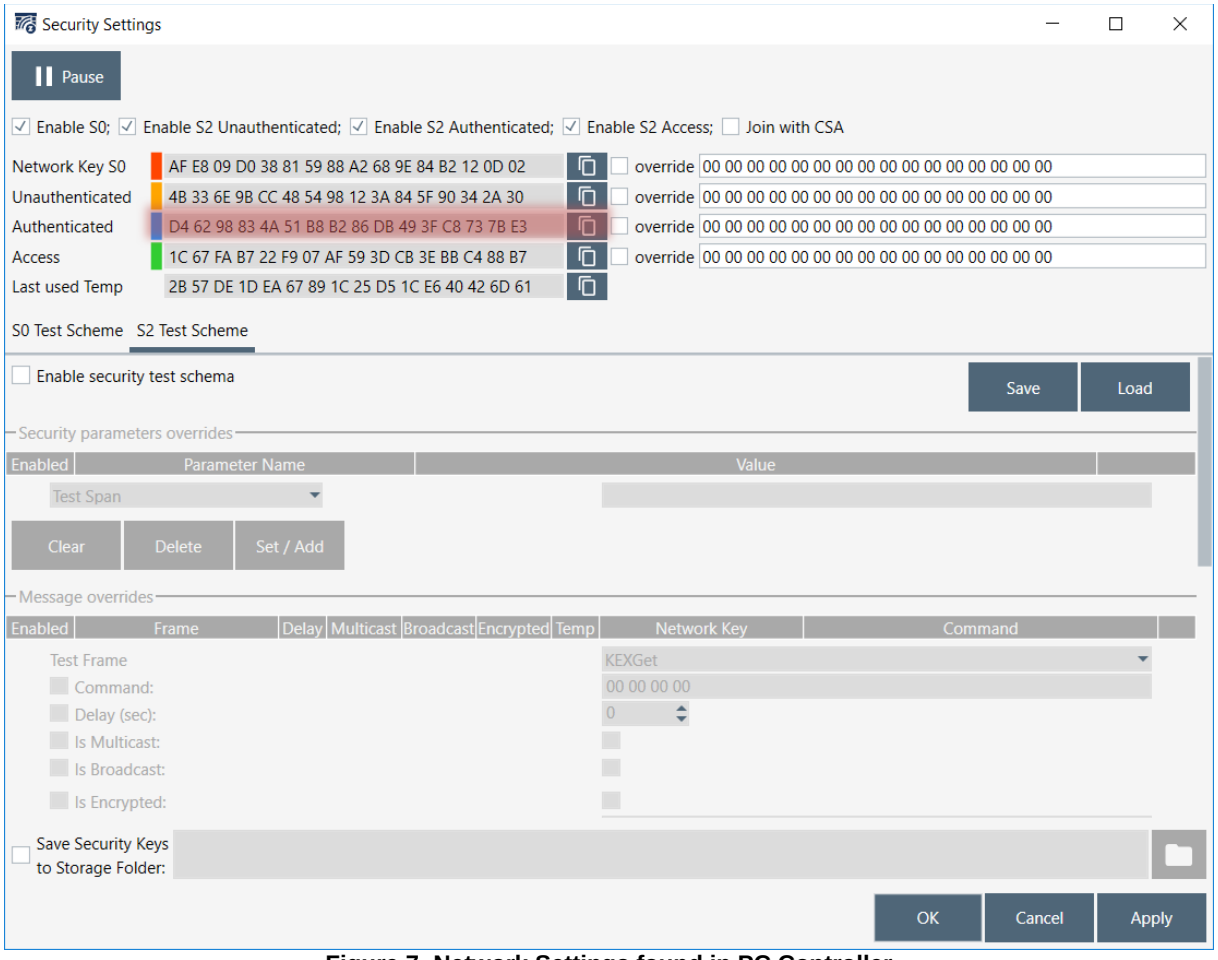

Figure 7: Network Settings found in PC Controller

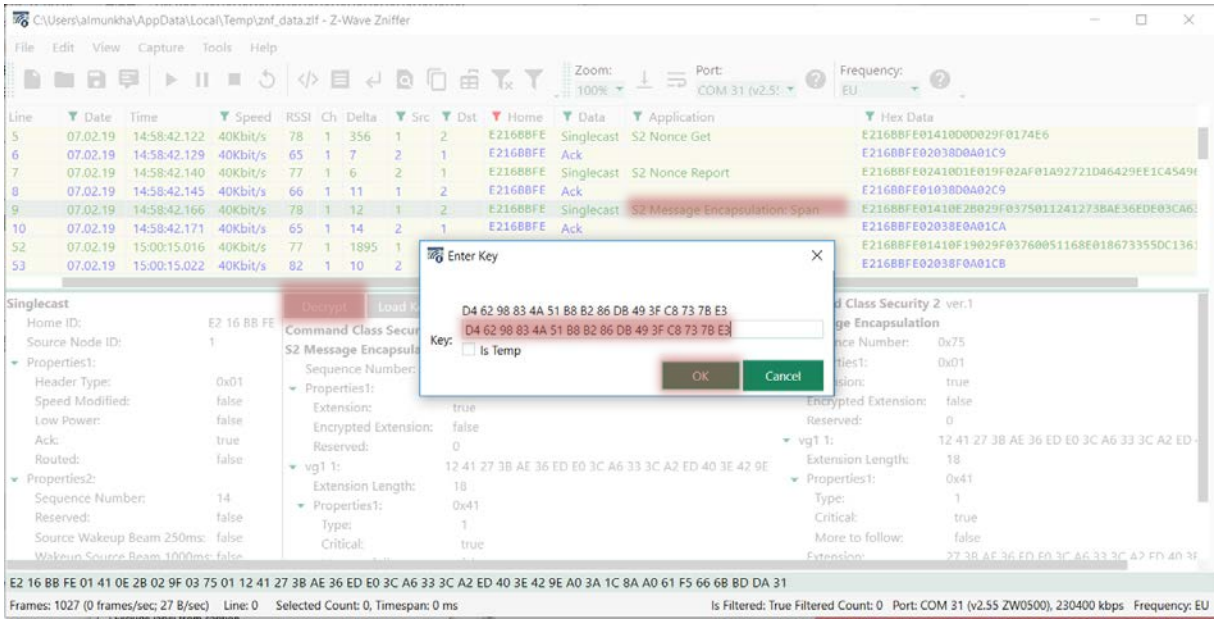

Figure 8: Enter Network Key in Zniffer

When the key is known, it is time to decrypt the traffic using the Zniffer.

1. Click on a S2 Message, refer to Figure 8.
2. Click on “Decrypt”
3. Paste the network key.
4. Click “OK”

With the SPAN synchronization and the network key, the Zniffer can now decrypt the S2 messages.

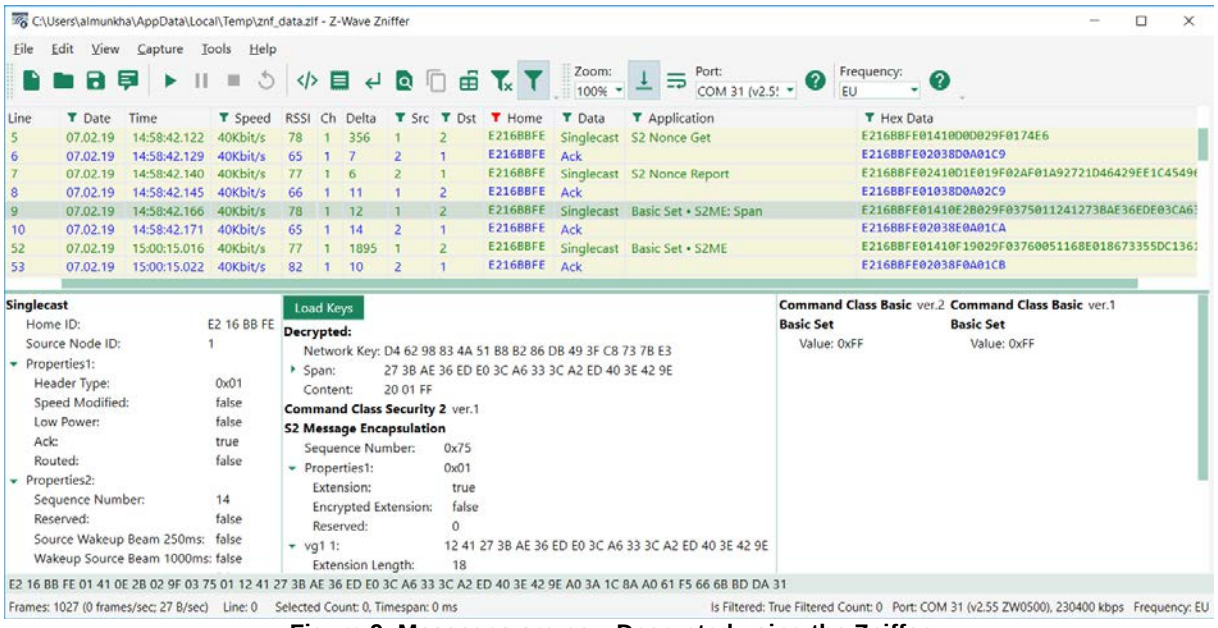

Figure 9: Messages are now Decrypted using the Zniffer

Notice how the 2 frames contains a Command Class called “Basic”, with command “Basic Set” and values “0xFF” (ON) and “0x00” (OFF).

Hint More information on the decrypting Z-Wave frames using the Zniffer be found the Knowledge Base:

Decrypt S2 frames in Zniffer trace

2.3 Using Command Class Binary Switch

When you send a Basic Set Command to the Switch On/Off, it is being mapped to the Binary Switch Command Class by the device. This is a requirement in the Z-Wave Specification for a Device Type of type “Binary Switch”.

Refer to Z-Wave specification SDS14224 Z-Wave Plus v2 Device Type Specification.

4.5.9.3 Basic Command Class Requirements

The Basic Command Class MUST be mapped according to Table 17.

Table 17, Binary Switch Device Type Basic mapping

Basic Command	Mapped Command
Basic Set (Value)	Binary Switch Set (Value)
Basic Report (Current Value, Duration)	Binary Switch Report (Value, Duration).

Figure 10: Basic Mapping for Device Type Binary Switch

The reason for this requirement is to ensure all Z-Wave controllers can do basic communication with all Z-Wave devices.

In this section, we will try to turn the LED ON and OFF using the Binary Switch command class.

1. In the PC Controller, double click on “25 – SWITCH_BINARY” under secure Command Classes in the lower left corner.
2. This opens the “Command Classes” view in the PC Controller and selects the Switch Binary Command class.

3. Set the Command to “0x01 – SWITCH_BINARY_SET”
4. Set the “Target Value” to “FF-ON_ENABLE”
5. Click “Send”.

6. Set the “Target Value” to “00-OFF_DISABLE”
7. Click “Send”.

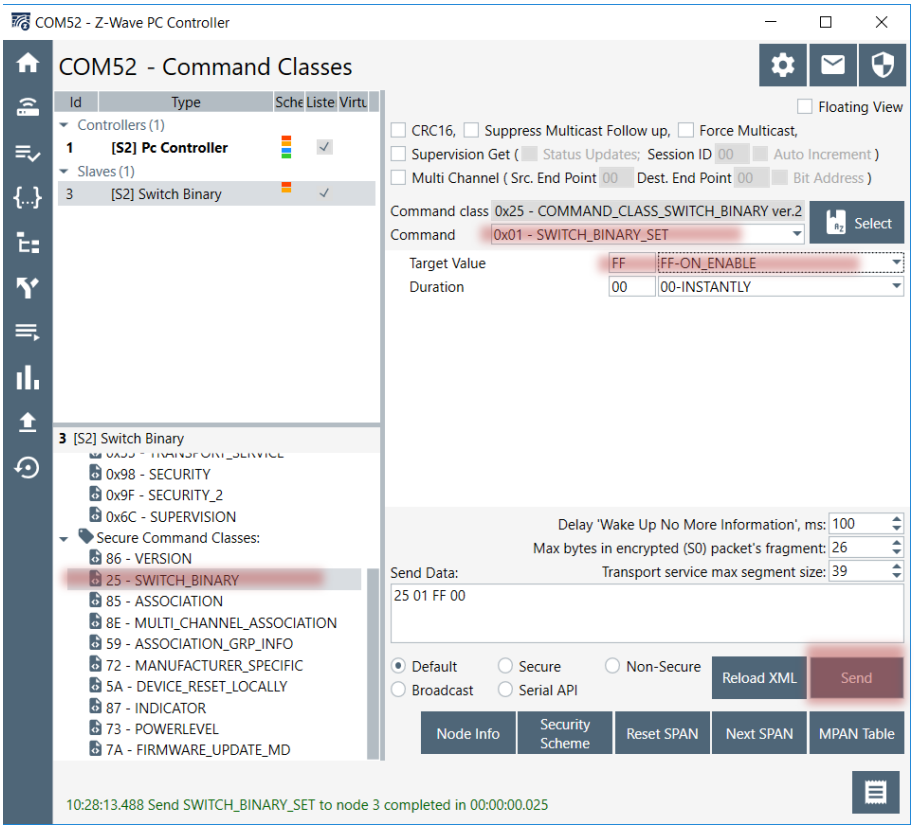

Figure 11: Command Class View in PC Controller

2.4 Capture RF packages using the Zniffer: Binary Switch Set

Now that we have learned how to send a Binary Switch Set, let's trace the RF communication again to understand which frames are being sent.

- Return to Z-Wave Zniffer tool, which should have been running in the background.
- The trace now contains a Nonce resync, 2 Basic Set frames and 2 Binary Switch Set frames.

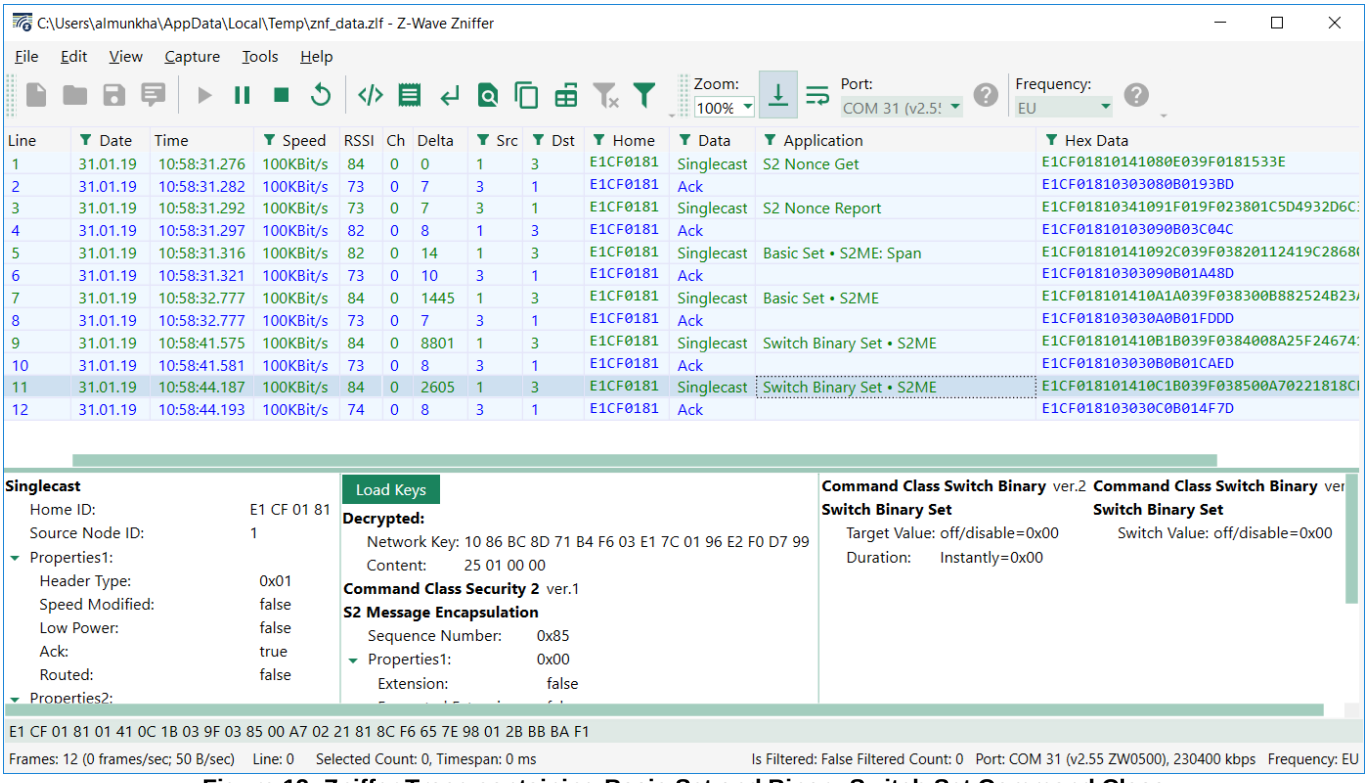

Figure 12: Zniffer Trace containing Basic Set and Binary Switch Set Command Class

Notice how to Zniffer shows the command class used to transfer data between the PC Controller and the device.

Now try to send a "Switch Binary Get" from the PC Controller, and see the response in the Zniffer.

- What does the response show?

This concludes the tutorial in how to trace and decrypt Z-Wave RF traffic using the Zniffer tool.