

# riscure

## What's new in Inspector 2018.1

SCA & FI  
software update  
January 2018



# Contents

Page 3	<b>Deep Learning</b>
Page 5	<b>Automation module</b>
Page 6	<b>Template attack for RSA</b>
Page 7	Piñata
Page 8	New Licensing model
Page 9	Known Key Analysis improvements
Page 11	Usability improvements
Page 15	Perturbation changes
Page 17	<b>Upgrade procedure &amp; SDK changes</b>
	<ul style="list-style-type: none"><li>• Inspector installation</li><li>• SDK changes</li></ul>

# Deep Learning

The Deep Learning module uses a convolutional neural network to make side channel analysis more efficient. Best results can be achieved with alignment, point of interest selection, classification of data and key recovery. The network that can be trained on a selection of a trace set and applied to the full trace set. The module will assist the user to choose the best configuration of hyper parameters.

- ✓ Boosts your SCA template analysis capabilities and rely on a neural network next to the expertise of your analyst to be successful.
- ✓ It is easy to train the network to the unique quirks of your trace acquisition process
- ✓ Extend 'human' research effort with processing power
- ✓ Be compliant: evaluation using Deep Learning algorithms has recently become a requirement for a number of common certification schemes.

Batch Sizes

Batch Size Train	Batch Size Validat...	Batch Size Test
<input type="text" value="0.6"/>	<input type="text" value="0.2"/>	<input type="text" value="0.2"/>

Parameters And Optimization

Define your sets

Hyper-Parameters Search

Convolutional Layers

Min	<input type="text" value="1"/>	Max	<input type="text" value="3"/>
-----	--------------------------------	-----	--------------------------------

Dense Layers

Min	<input type="text" value="1"/>	Max	<input type="text" value="3"/>
-----	--------------------------------	-----	--------------------------------

Convolutional Filters

Configure network layers

Initial Parameters

Convolutional Layers	<input type="text" value="1"/>
Dense Layers	<input type="text" value="1"/>
Convolutional Filters	<input type="text" value="9"/>
Number of Neurons	<input type="text" value="9"/>
Number Of Iterations	<input type="text" value="1"/>
Number Of Epochs	<input type="text" value="50"/>
Learning Rate (*0.001)	<input type="text" value="50"/>
Regularization Value (*0.00001)	<input type="text" value="1"/>
Activation ConvLayer	<input type="text" value="relu"/>
Activation DenseLayer	<input type="text" value="tanh"/>
Activation OutputLayer	<input type="text" value="softmax"/>
Loss Function	<input type="text" value="negativeLikelihood"/>

Automate hyper parameter search

# Deep Learning

Cipher Settings

Cipher

Cipher

Operation

Key

☐ Get key from data

Works both for DES and AES ciphers. The module can be trained with a known key that you set for all the traces or with a variable known key which is stored inside the data section of the traces. Applying your trained network can be done on a trace set with an unknown key!

Number of Dense Layers

Dense Layer 1

Number of Neurons

Activation Dense Layer

Define the number of dense layers that you will need to optimize the performance of your network. You can choose to have the number of neurons and the activation method the same for all the layers or vary per layer if needed to get better results

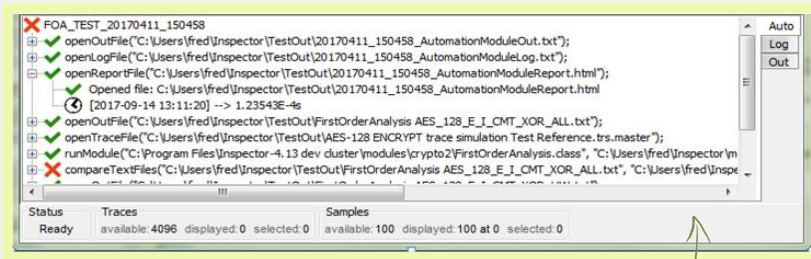
☐ Early Stopping

Training your network can be time consuming. To assist with searching for the best network parameters in a limited amount of time, we have added an early stopping option. Check this option and set your time limit. The module will search for the best configuration within this timeframe!

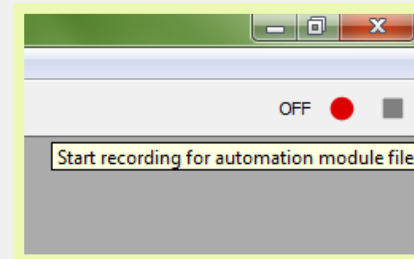
# Automation

This new module enables you to reduce manual work and perform side channel analysis faster than ever before. Use record and playback functions to create a test scenario once and run it multiple times without the need for repetitive actions. The module enables regression testing and archives everything used in a scenario: parameters, templates, intermediate results, reference traces, etc.

- ✓ Generates a programmable user module
- ✓ Build loops to run a automation scenario with multiple settings
- ✓ Works with all modules
- ✓ Integrates perfectly with Inspector High Performance Analysis (HPA)
- ✓ Uses known Inspector principles to guarantee a steep learning curve for users



Progress of the automation scenario is shown in new “auto” tab



Buttons enable ‘macro like’ recording of automation scripts

# Template attack for RSA

Known-key template analysis for public key operations on RSA SFM tutorial + Pattern extracted(2) + Sta...

Samples  
First: 0  
Number: 79000

Traces  
First: 773  
Number: 7735

Template analysis settings  
Phase  
☐ Learn ☒ Apply  
Model  
☒ Mean ☐ +Var ☐ +Cov  
Optimiser  
☒ None ☐ Pooled

Target settings  
Trace type bits: 1  
Trace type offset: 0

Learn phase settings  
Report interval: 0  
Generate traces: ☐  
Points of interest  
ist\target\inspector-code-dist\pointsofinterest.poi Browse  
Templates file  
ode-dist\target\inspector-code-dist\rsa.templates Browse

Apply phase settings  
Report interval: 0  
Points of interest  
nspector-code-dist\pointsofinterest.poi Browse Copy  
Templates file  
rget\inspector-code-dist\rsa.templates Browse Copy  
Save detailed results to file  
results.txt Browse  
Results Processor  
Pinata RSA SFM Square and Multiply

- ✓ New template analysis module allows user to classify traces containing different operation types from a public key implementation
- ✓ User selectable results processor
- ✓ User can develop new results processors for custom implementations using the module wizard

Operations that are used for template attacks on DES and AES also apply for RSA

# Piñata



- ✓ Piñata 2.1 release support RSA SFM decrypt commands
- ✓ New sequence can be used for acquisition to demonstrate Template Analysis on RSA
- ✓ New sequence has an option to select different RSA implementations on target
- ✓ Two SM4 implementations supported

Samples		Traces	
First:	0	First:	0
Number:	2800	Number:	500

Settings		Cipher	
Candidates in output:	4	Cipher:	SM4 (beta)
Report interval:	0	Preferences:	Mode: ENCRYPT
Generate traces:	<input checked="" type="checkbox"/>		
Method:	Correlation		
Preferences:	<input type="checkbox"/> Amplified		
Cross correlation:	None		

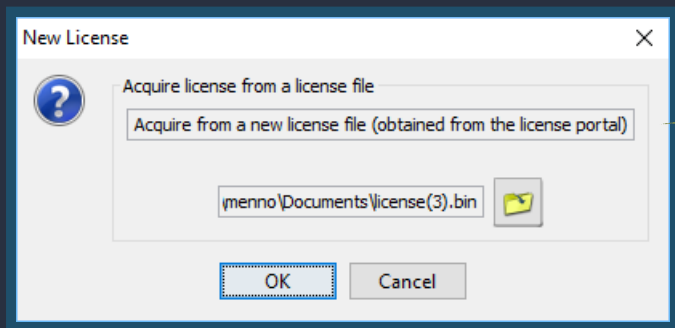
SM4 supported in analysis modules



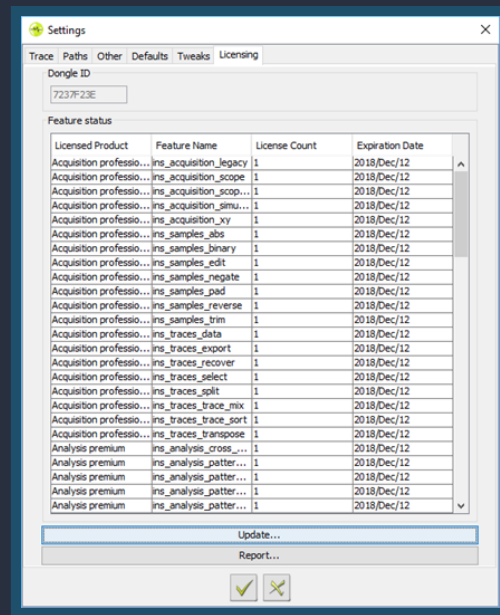
# New licensing model

Inspector 2018.1 works with a new licensing model. To work with this Inspector release, you have to use your dongle and a license file. You will receive this license file from Riscure.

The new licensing model will also allow for trial licenses so you can test features for some time before you decide to purchase. Please check with your account manager for options and availability.



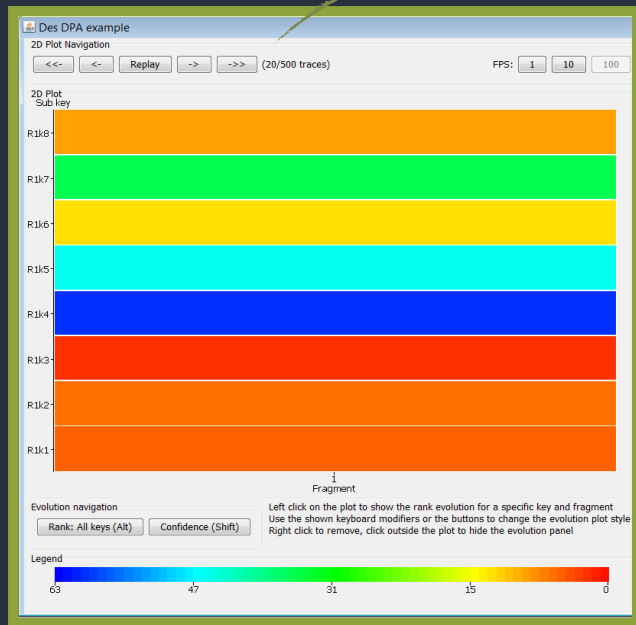
Place you license file in the Inspector user directory and import it using the update button from the licensing tab in the settings menu



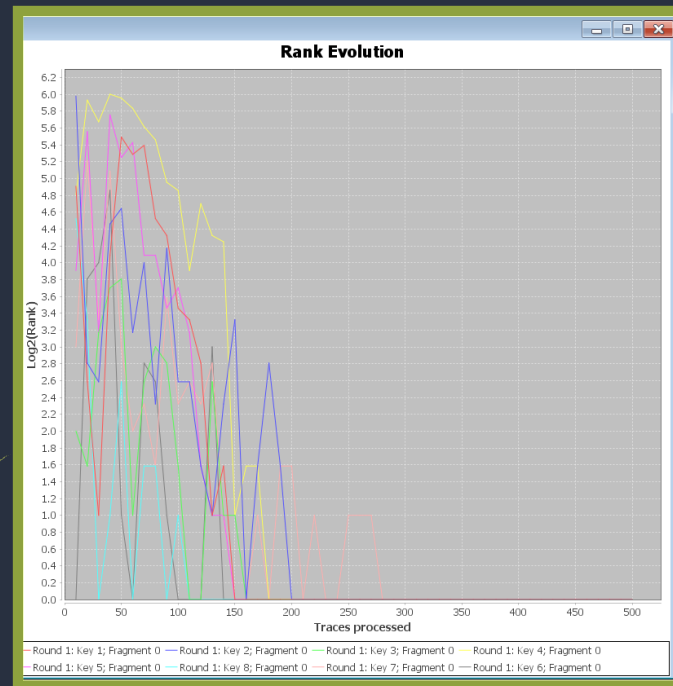
The new licensing tab that you can access from the settings menu will show all the modules that are available within your software package as well as the license ID of your dongle



# Known Key Analysis



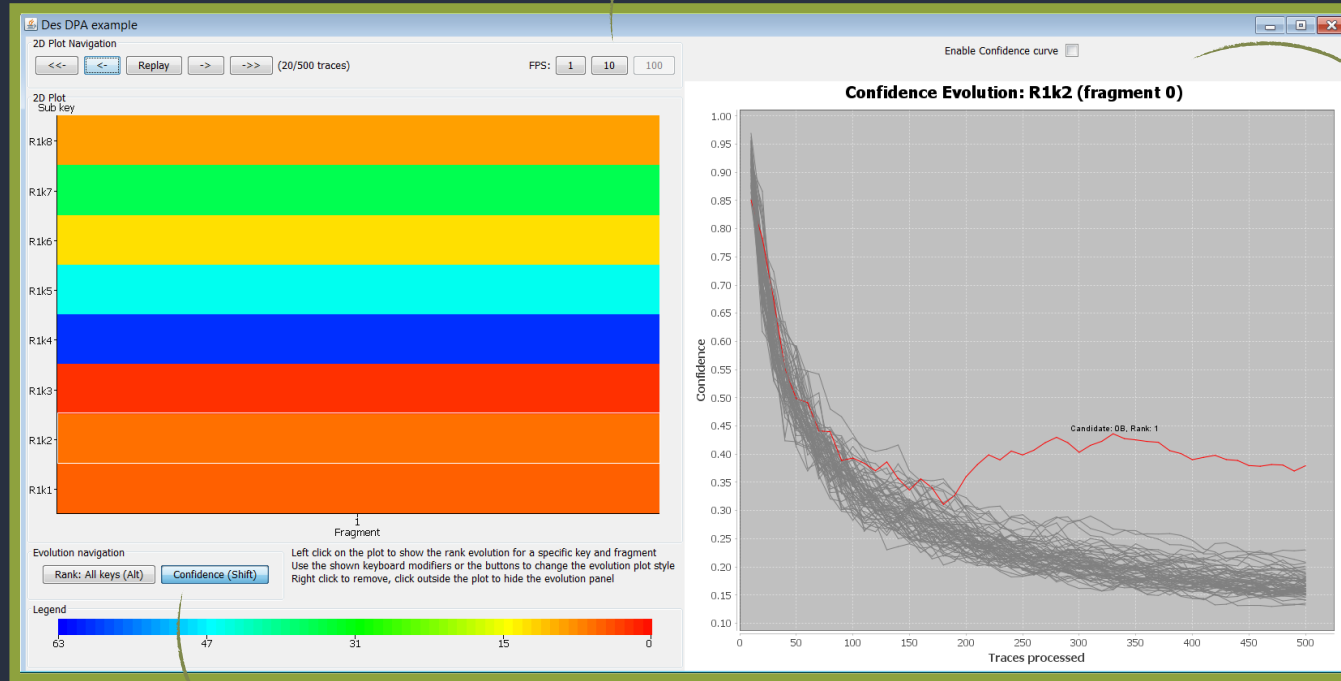
Scroll through your selected report interval to see results changing over time



Get a clear overview of all key byte ranking evolution for the round you selected.

# Known Key Analysis

Replay the attack to see the charts evolving during the attack. You are able to set the replay speed from within the chart

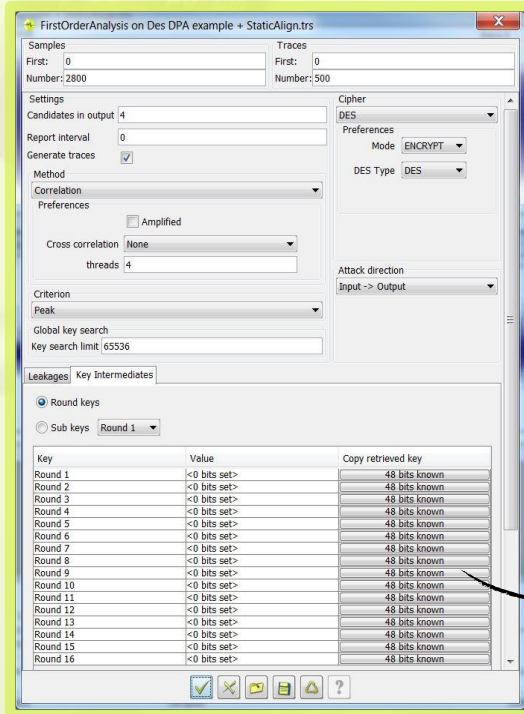


The diagram will show the confidence evolution for each sub key of the selected round. Select a sub key in the plot to change the confidence diagram

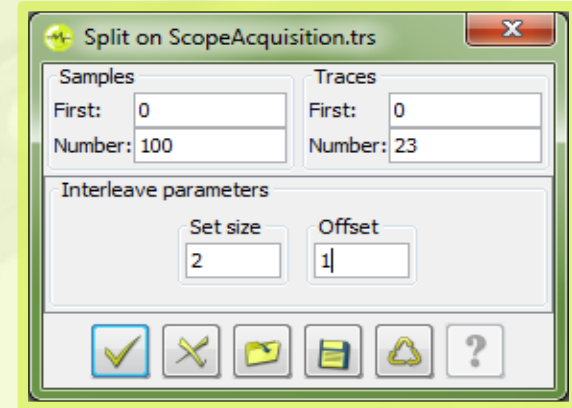
Switch between key ranking and confidence

# Usability improvements

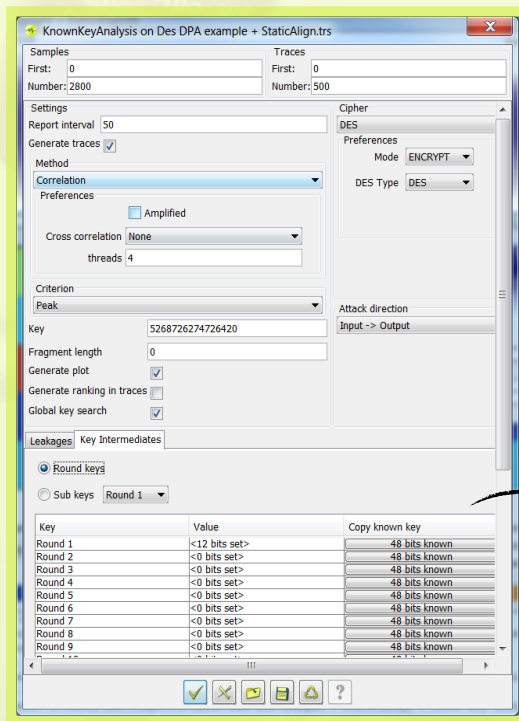
Split settings are stored and last used values will appear upon next usage



DES intermediate sub keys show 48 bits and can be easily copied



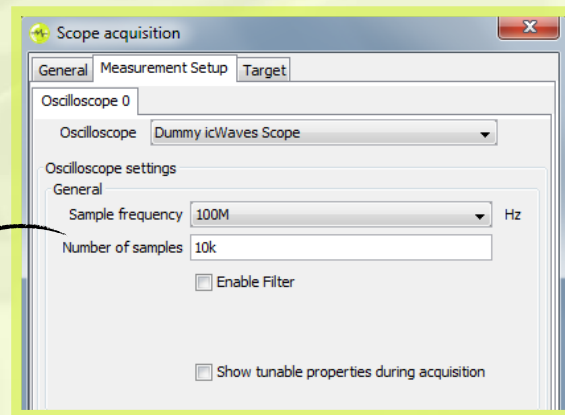
# Usability improvements



Partial Known  
Key Analysis  
is possible

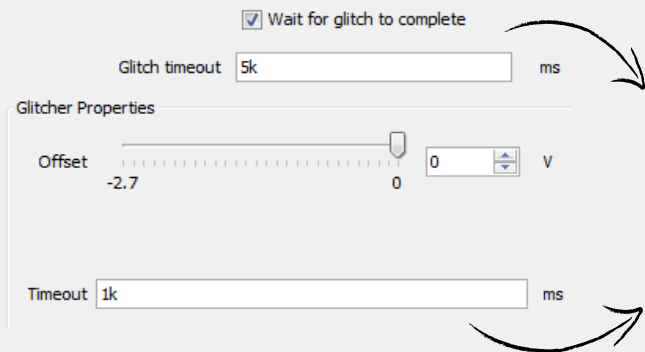
All scopes now have  
default number of  
samples set to 10,000  
samples

New 'Copy known key' column for KKA  
(Similar to FOA panel, but always  
enabled – since all bits are known)



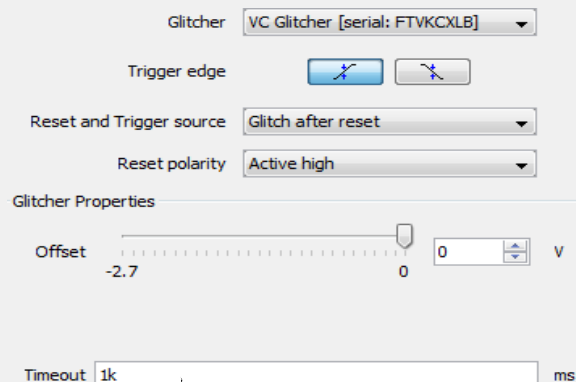
# Simplified VC Glitcher timeout

Inspector 4.12 and earlier



When using embedded perturbation modules, users were presented with 2 VC Glitcher timeouts.

Inspector 2018.1

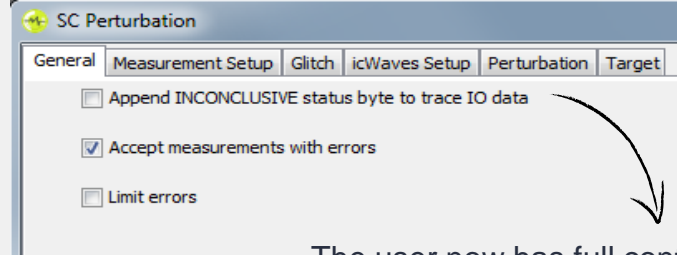


The user has one option to configure a timeout. Inspector will take care of the USB transfer timeout, which is irrelevant to the FI operation.

# Inconclusive byte

Value	Data
1.22464685E-17 at 50 (500 µs)	A6 9B 24 47 09 08 FE F6 25 AB 53 98 CA 62 C7 3A 01

An extra byte was always appended to trace data from any perturbation module. It signals the status of corresponding perturbation attempt.



The user now has full control to add an additional byte or not through Inspector. In this way the byte is only appended when it's useful (e.g. AES, DES DFA modules).



# Perturbation log changes

Result count added to view  
and database

Editable description field

Timestamp  
added to module  
log

The screenshot shows a window titled "Open Log" with a table of log entries and a detailed log view on the right. The table has columns: Module name, Start time, Status, Result count, and Description. The detailed log view shows a timestamp [2017-05-11 15:46:23] and the following text:

```
[2017-05-11 15:46:23]
Module executed: SC Perturbation
Module class path: C:/Users/job/Document
Input trace: <none>
Parameters:
{first.trace=0, number.of.samples=0, fir
Output file name: G:\data\~SC Perturbati
Runtime (s): 4.143149352
Traceset result: G:\data\~SC Perturbatio
```

At the bottom of the window are buttons: Open, Delete, Cancel, and Export.

Module name	Start time	Status	Result count	Description
DES perturbatio...	2017-05-12 10:...	Finished	1	
DES triggered p...	2017-05-12 10:...	Pending	0	
RC_TC2_Protoc...	2017-05-11 16:...	Finished	10	
RC_TC6_Protoc...	2017-05-11 16:...	Finished	10	system crashed
RC_TC2_Protoc...	2017-05-11 16:...	Finished	10	
RC_TC2_Protoc...	2017-05-11 16:...	Finished	10	
RC_TC6_Protoc...	2017-05-11 15:...	Finished	10	
RC_TC6_Protoc...	2017-05-11 15:...	Finished	0	
RC_TC2_Protoc...	2017-05-11 15:...	Finished	10	the best one yet
RC_TC2_Protoc...	2017-05-11 15:...	Finished	10	
RC_TC6_Protoc...	2017-05-09 11:...	Finished	10	
PinataAESdecry...	2017-04-18 13:...	Finished	5	
RC_TC6_Protoc...	2017-04-18 13:...	Finished	10	
RC_TC6_Protoc...	2017-04-18 13:...	Finished	10	
RC_TC6_Protoc...	2017-04-18 13:...	Finished	42	test
RC_TC6_Protoc...	2017-04-18 13:...	Finished	47	
PinataAESdecry...	2017-04-14 16:...	Finished	5	
PinataAESdecry...	2017-04-14 16:...	Finished	5	
RC_TC2_Protoc...	2017-04-14 16:...	Finished	64	
RC_TC2_Protoc...	2017-04-14 16:...	Finished	800	

Export will give you an option to export  
result into a sqlite database

# Perturbation log changes

VC Glitcher report - RC\_TC2\_Protocol\_SC Perturbation (started 2016-09-19 08:27:59)

id	Glitch voltage	VCC voltage	Clock high ...	Clock low v...	Wait cycles 1	Glitch cycle...	Glitch offs...	Glitch lengt...	Timed out	Data
20	2.46600008...	3.29900002...	3.29900002...	0.0	1000	40	354	60	false	00 00 0E A0 04 00 00 00 11 7F 28 CA 0A 54 2E 3C 08 22 38 E7 08 FF E1
19	1.96000003...	3.29900002...	3.29900002...	0.0	1000	46	218	94	false	00 00 0E A0 04 00 00 00 29 89 21 42 D5 02 81 24 08 15 00 00 A9 3C C6 4
18	2.64000010...	3.29900002...	3.29900002...	0.0	1000	72	436	10	false	00 40 0E A0 04 00 00 00 0E 1C CC D6 D6 72 E2 1E 08 8A 00 40 0A 58 79 6
17	2.26200008...	3.29900002...	3.29900002...	0.0	1000	7	430	38	false	00 00 0E A0 04 00 00 00 C9 21 F8 06 F5 5A 83 69 08 C9 00 00 0A EA 0F 5
16	2.46000003...	3.29900002...	3.29900002...	0.0	1000	57	518	34	false	00 40 0E A0 04 00 00 00 EB 04 F9 06 83 F4 48 9F 08 E2 00 40 0A 03 E5 3
15	0.81599998...	3.29900002...	3.29900002...	0.0	1000	3	444	12	false	00 00 0E A0 04 00 00 00 8A 3A 3E 4A D8 D7 43 CE 08 D8 00 00 0A 3E E7 0
14	1.55799996...	3.29900002...	3.29900002...	0.0	1000	44	318	68	false	00 40 0E A0 04 00 00 00 38 08 04 F5 34 77 14 5A 08 96 00 40 0A C8 02 0
13	0.77999997...	3.29900002...	3.29900002...	0.0	1000	69	276	96	false	00 00 0E A0 04 00 00 00 79 FD 88 D9 6D 89 E6 9C 08 E1 00 00 0A 0A F7 0
12	0.81999999...	3.29900002...	3.29900002...	0.0	1000	41	232	14	false	00 40 0E A0 04 00 00 00 12 C8 4C 7E AF 73 F9 7E 08 59 00 40 0A 0A 02 0
11	0.74199998...	3.29900002...	3.29900002...	0.0	1000	74	354	82	false	00 00 0E A0 04 00 00 00 7F 30 FA 58 F1 51 40 F5 08 5C 00 00 0A 0A 02 0
10	0.23399999...	3.29900002...	3.29900002...	0.0	1000	48	362	14	false	00 40 0E A0 04 00 00 00 D2 67 5C 84 97 87 6E 10 08 D9 00 40 0A A5 46 4
9	2.20000004...	3.29900002...	3.29900002...	0.0	1000	11	806	68	false	00 00 0E A0 04 00 00 00 00 4A D9 3A 12 CF A0 BD 08 CE 00 00 0A 0A 28 6
8	-1.0240000...	3.29900002...	3.29900002...	0.0	1000	24	190	80	false	00 40 0E A0 04 00 00 00 F3 66 A8 C7 F1 F3 3C EE 08 C3 40 0A 0A 18 61 6
7	0.29399999...	3.29900002...	3.29900002...	0.0	1000	84	128	58	false	00 00 0E A0 04 00 00 00 36 2E BC DC EC EC 99 08 08 40 00 0A 7F 36 8
6	1.78199994...	3.29900002...	3.29900002...	0.0	1000	4	950	100	false	00 40 0E A0 04 00 00 00 44 85 87 D1 D5 98 C8 5C 08 97 00 40 0A A2 19 9
5	1.44400000...	3.29900002...	3.29900002...	0.0	1000	17	486	70	false	00 00 0E A0 04 00 00 00 2C 64 25 12 68 EF FF 97 08 3A 00 00 0A 0A 04 F
4	-1.1160000...	3.29900002...	3.29900002...	0.0	1000	74	642	0	false	00 40 0E A0 04 00 00 00 4E 8C 9C FA 73 8F 65 13 08 C4 00 40 0A D6 3C 3
3	0.75999999...	3.29900002...	3.29900002...	0.0	1000	88	410	64	false	00 00 0E A0 04 00 00 00 CE CE 4A 2F D7 D7 82 96 08 C1 00 00 0A C5 88 5
2	0.88200002...	3.29900002...	3.29900002...	0.0	1000	44	612	10	false	00 40 0E A0 04 00 00 00 07 1A 29 D8 48 4F 84 9F 08 19 00 40 0A 3F A8 6
1	0.85199999...	3.29900002...	3.29900002...	0.0	1000	85	276	40	false	00 00 0E A0 04 00 00 00 71 34 9F 28 D5 3C 4C 85 08 78 00 00 0A E4 99 4
0	0.38600000...	3.29900002...	3.29900002...	0.0	1000	96	126	52	false	00 E7 08 FF E1 31 FE 45 52 69 73 63 75 72 E5 5A 00 00 0C 00 A4 04 00 0

Filter expression: "Color" = <img alt="color icon" data-bbox="115 645 130 660"/> <br/> Rows: 21 <span>ASCII/Hex</span>

Smaller fonts

Previously used filter expressions are saved and accessible through a drop-down with history

Context menu is available to apply filters in an easy to understand way

Filters for - RC\_TC2\_Protocol\_SC Perturbation (started 2016-09-19 08:27:59)

If (Glitch length 1) equals [ ] then [Include]

Reset Add Remove

Column	Value	Action
Glitch length 1	100	INCLUDE

Ok Apply Cancel



# Upgrade procedure & SDK changes



# Inspector installation & SDK updates

## Where

- Customers with a Subscription Contract receive a download link
- Download from Riscure license portal

## Installation guidance

- Inspector software can be installed on the same PC workstation next to your previous version. You can still revert back to the previous version if you want to.
- You will need a license file next to your dongle to work with Inspector 2018.1.
- API is backwards compatible.

## Your own modules & traces

- Inspector software points by default to the same user module folder as previous versions.
- In case you have trouble porting an older module to this Inspector version, please contact our support portal for assistance.

## Release notes & bug fixes

For the full list of bug fixes, please refer to the release notes:

<https://www.riscure.com/security-tools/inspector-sca/#support>

## SDK and firmware updates

### Spider SDK 1.4.0

- "waitTrigger" method in Chronology class now returns an integer id. User can use this id to determine which "waitTrigger" method timed out.
- Timer class is now available in Python

### icWaves SDK 3.10.0

- icWaves firmware 3.2.1, with an adjusted ADC chip configuration routine to ensure ADC sample encoding format
- Fixed an issue where icWaves3 ADC chip does not receive correct configuration and produces samples in an unexpected encoding format.
- Corrected the maximum number of samples parameter for icWaves1 devices to 1000000

### Power Tracer SDK 1.4.1

- SDK automatically performs volatile FPGA bit stream update when detected a device with older bit stream version

**Riscure B.V.**

Frontier Building, Delftechpark 49  
2628 XJ Delft  
The Netherlands  
Phone: +31 15 251 40 90

[www.riscure.com](http://www.riscure.com)

---

**Riscure North America**

550 Kearny St., Suite 330  
San Francisco, CA 94108 USA  
Phone: +1 650 646 99 79

[inforequest@na.riscure.com](mailto:inforequest@na.riscure.com)

---

**Riscure China**

Room 2030-31, No. 989, Changle Road, Shanghai 200031  
China  
Phone: +86 21 5117 5435

[info@cn.riscure.com](mailto:info@cn.riscure.com)

# riscure

## Challenge your security