riscure

What's new in Inspector 2018.1

SCA & FI
software update
January 2018

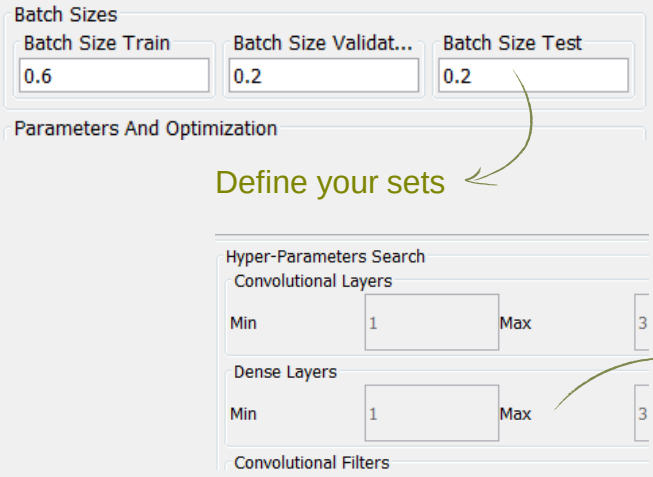
Contents

- Inspector installation
- SDK changes

Deep Learning

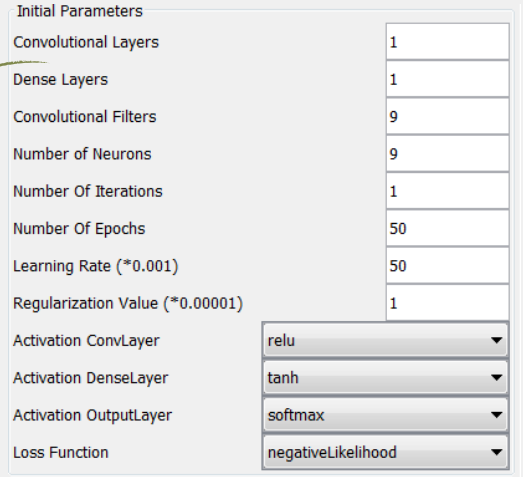
The Deep Learning module uses a convolutional neural network to make side channel analysis more efficient. Best results can be achieved with alignment, point of interest selection, classification of data and key recovery. The network that can be trained on a selection of a trace set and applied to the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

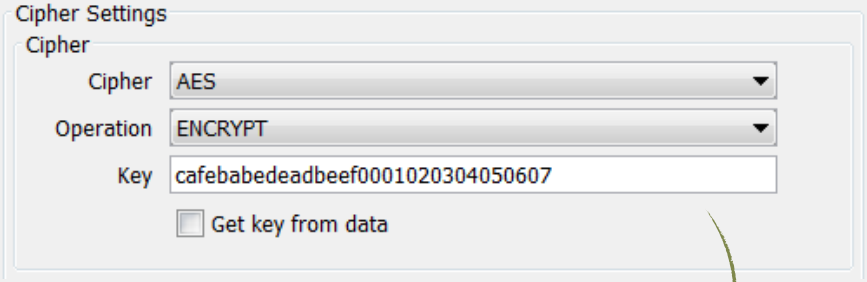


Automate hyper parameter search

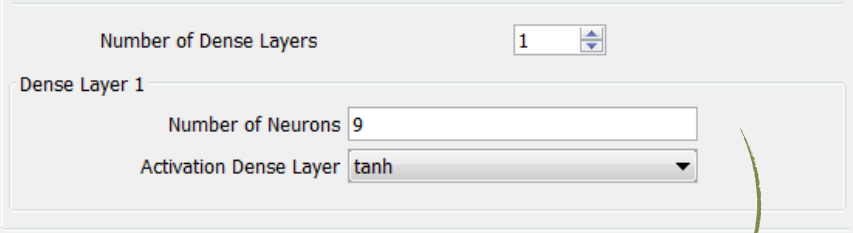
Configure network layers



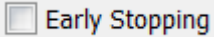
Deep Learning



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!



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

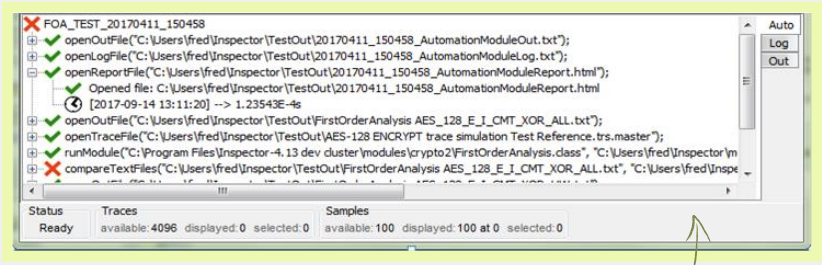


Training your network can be time consuming. To assist with searching for the best network parameters in a limited amount of time, we have added an early stopping option. Check this option and set your time limit. The module will search for the best configuration within this timeframe!

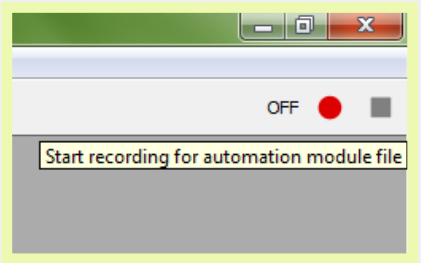
Automation

This new module enables you to reduce manual work and perform side channel analysis faster then 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

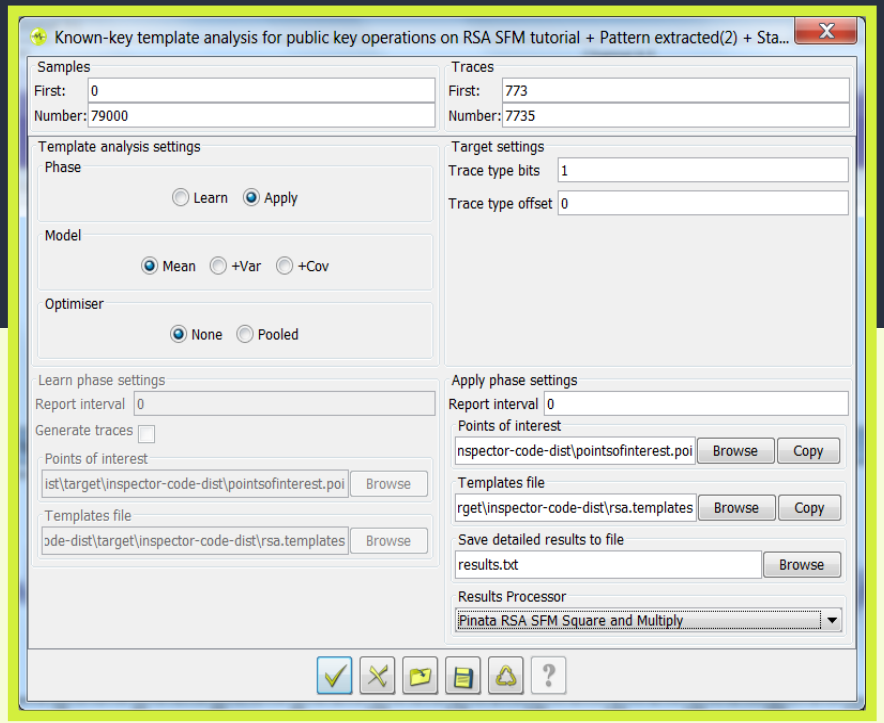


Progress of the automation scenario is shown in new “auto’ tab



Buttons enable ‘macro like’ recording of automation scripts

Template attack for RSA

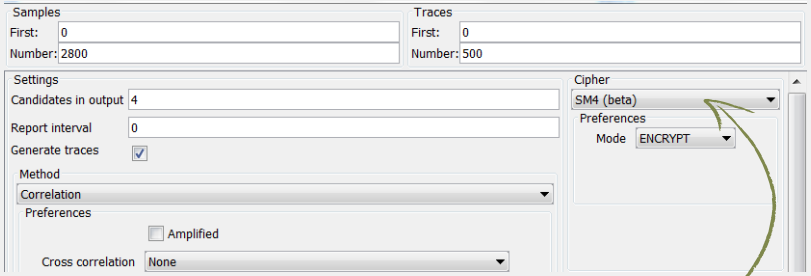


- ✓ New template analysis module allows user to classify traces containing different operation types from a public key implementation
- ✓ User selectable results processor
- ✓ User can develop new results processors for custom implementations using the module wizard

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



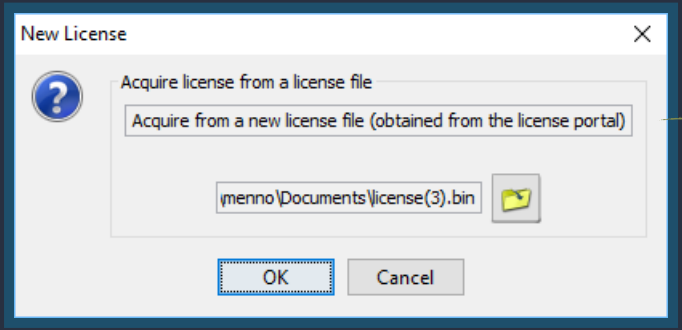
SM4 supported in analysis modules

riscure

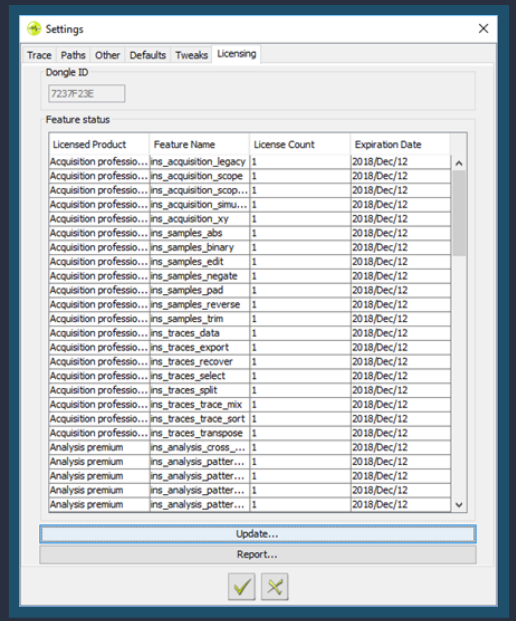
New licensing model

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.

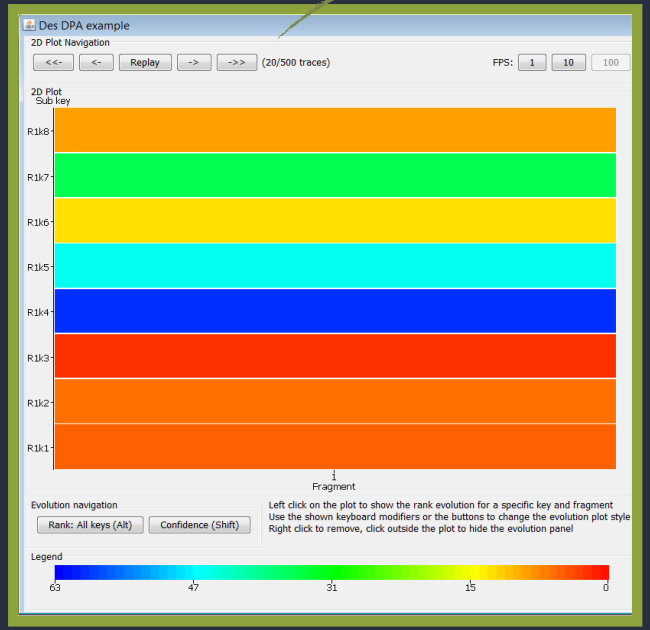


Place you license file in the Inspector user directory and import it using the update button from the licensing tab in the settings menu

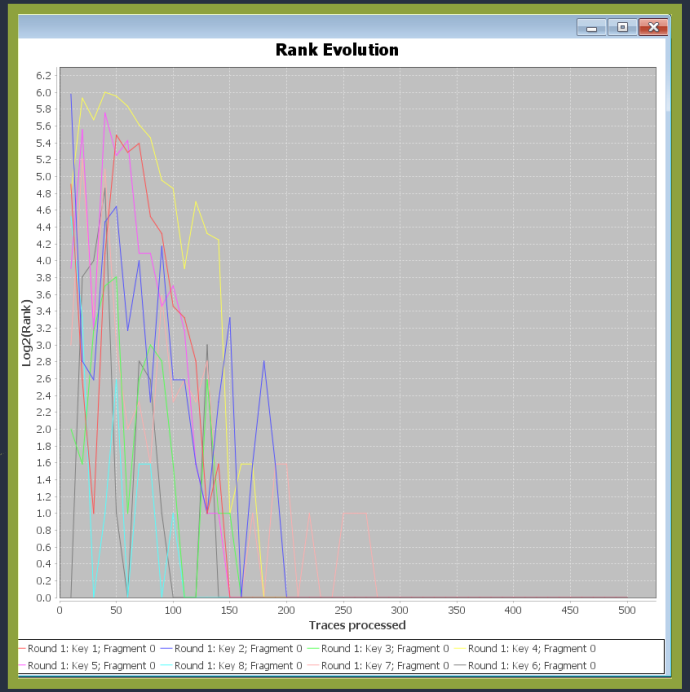


The new licensing tab that you can access from the settings menu will show all the modules that are available within your software package as well as the license ID of your dongle

Known Key Analysis



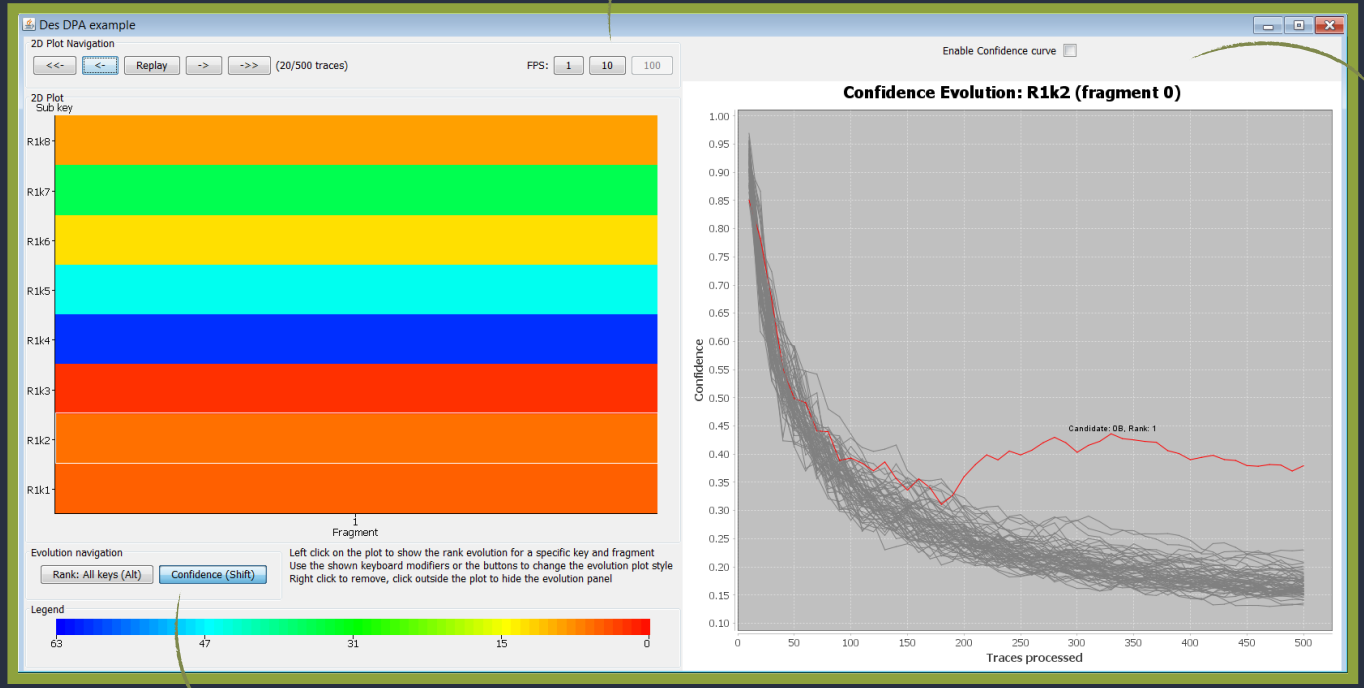
Scroll through your selected report interval to see results changing over time



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

Known Key Analysis

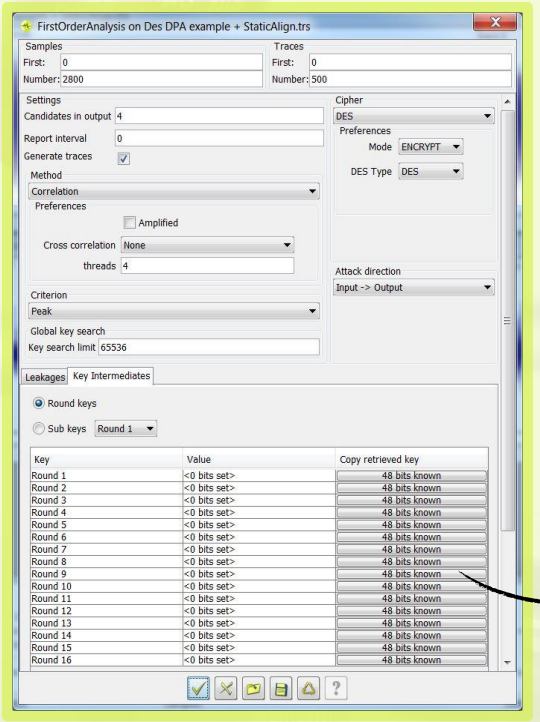
Replay the attack to see the charts evolving during the attack. You are able to set the replay speed from within the chart



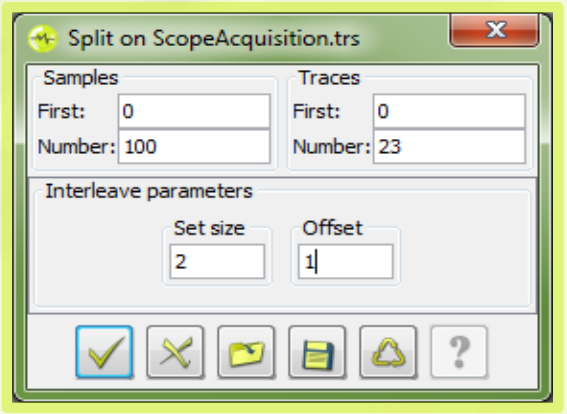
The diagram will show the confidence evolution for each sub key of the selected round. Select a sub key in the plot to change the confidence diagram

Switch between key ranking and confidence

Usability improvements

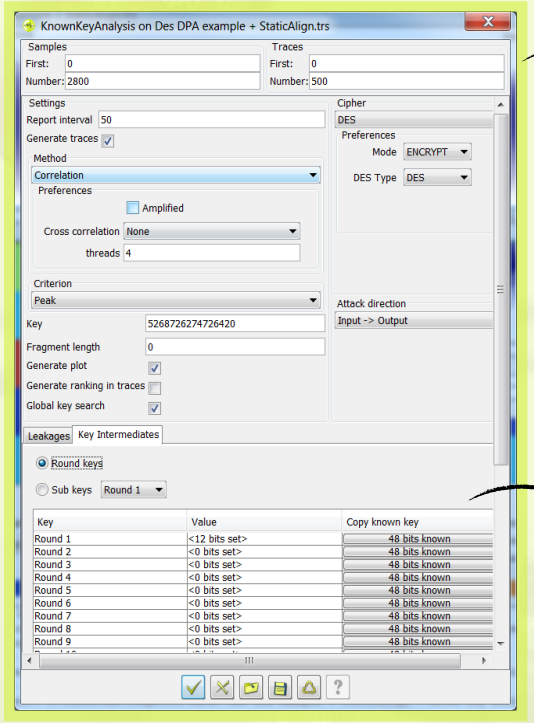


Split settings are stored and last used values will appear upon next usage

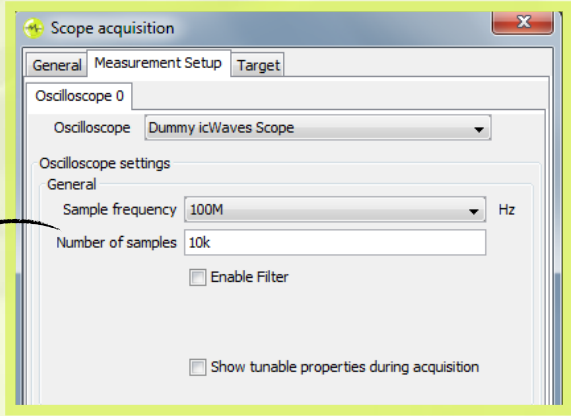


DES intermediate sub keys show 48 bits and can be easily copied

Usability improvements



Partial Known Key Analysis is possible

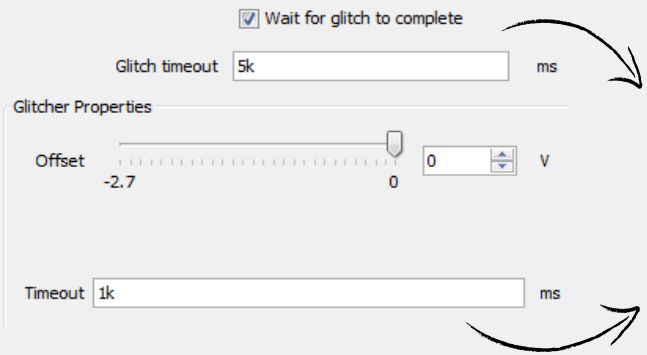


All scopes now have default number of samples set to 10,000 samples

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

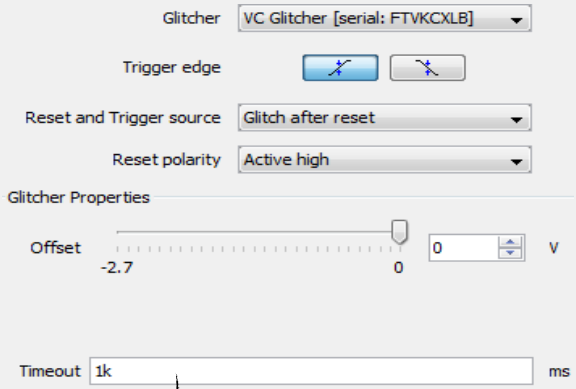
Simplified VC Glitcher timeout

Inspector 4.12 and earlier



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

Inspector 2018.1

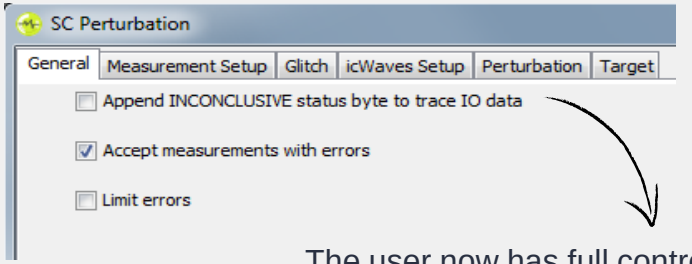


The user has one option to configure a timeout. Inspector will take care of the USB transfer timeout, which is irrelevant to the FI operation.

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.



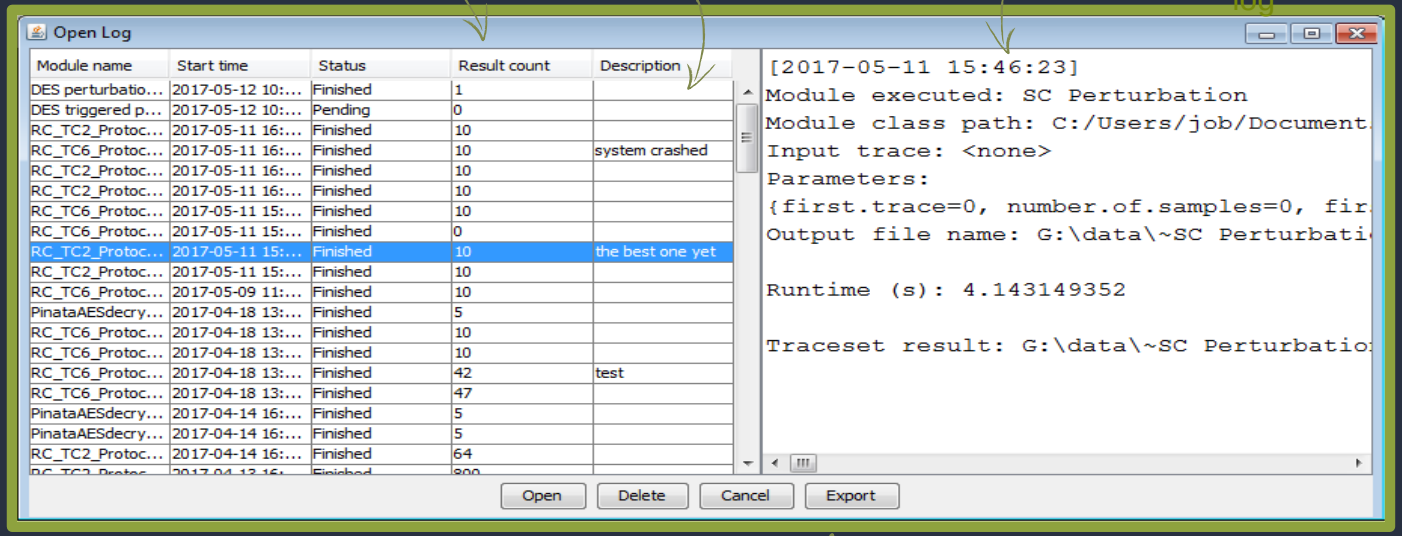
The user now has full control to add an additional byte or not through Inspector. In this way the byte is only appended when it's useful (e.g. AES, DES DFA modules).

Perturbation log changes

Result count added to view and database

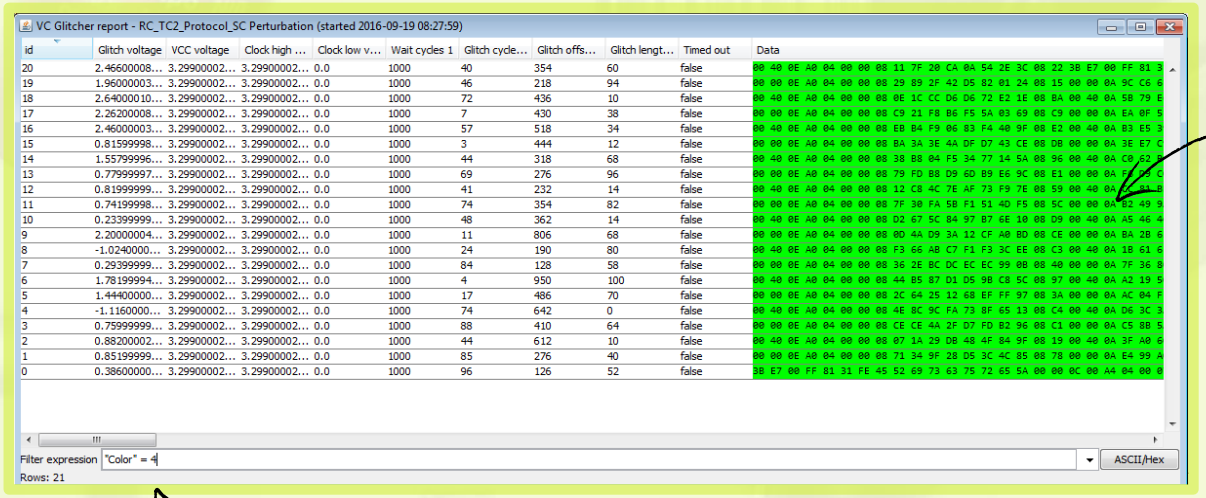
Editable description field

Timestamp added to module log



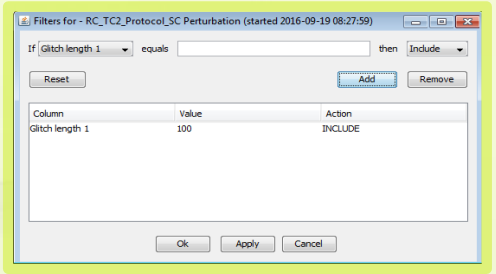
Export will give you an option to export result into a sqLite database

Perturbation log changes



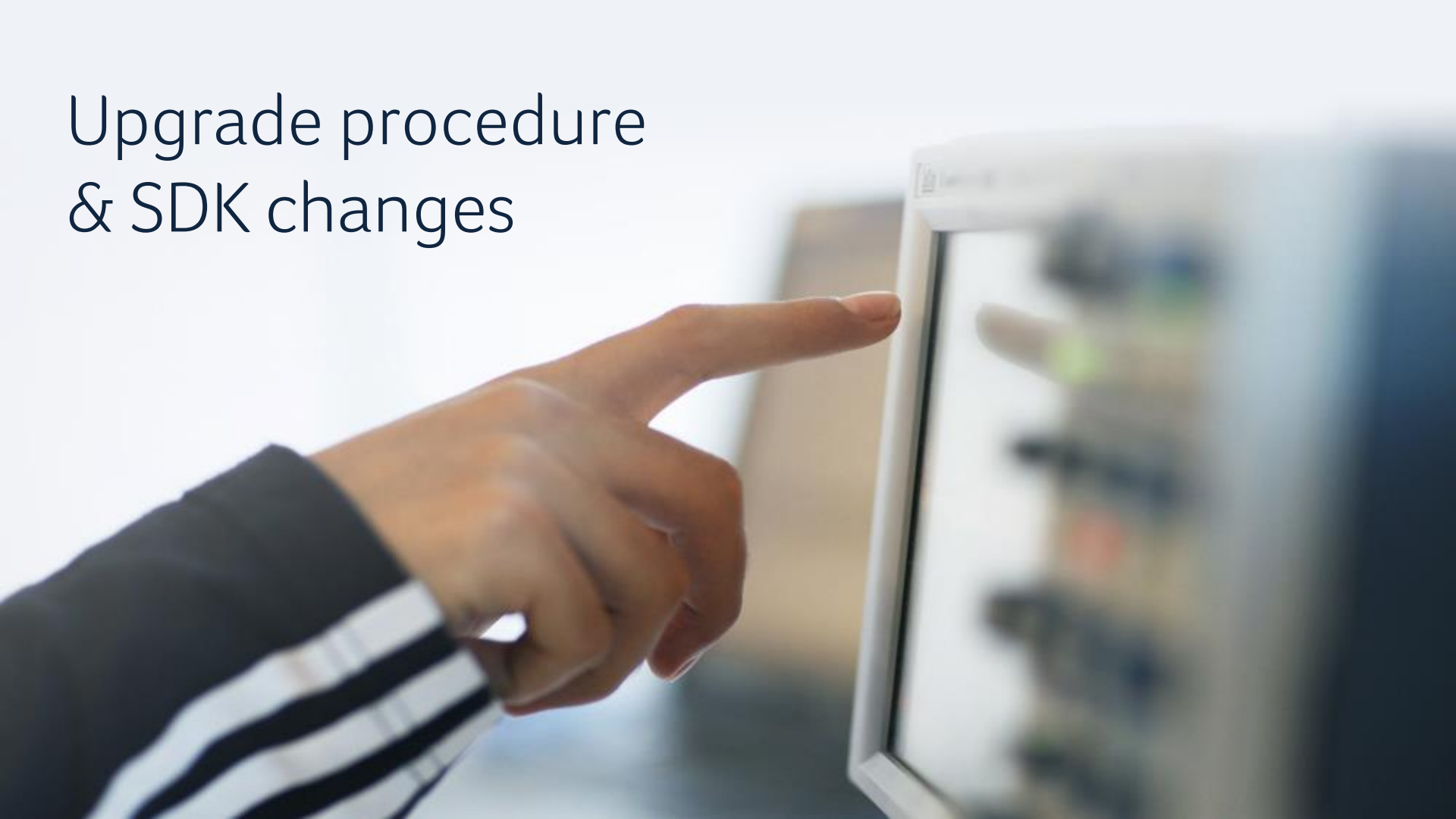
Smaller fonts

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

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 i cWaves1 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

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

inforequest@na.riscure.com

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

inforcn@riscure.com

riscure

Challenge your security