

CSA-Rainbow-Table-Tool-V2 Documentation

17.08.2013 (Version 1.00) up-to-date version on <http://colibri-dvb.info>
Colibri <colibri.dvb@googlemail.com>

Introduction

Nearly all encrypted digital television programs transmitted via satellite are scrambled by the CSA algorithm. CSA is used to encrypt the video and/or audio. The BISS encryption use a more or less static CSA key. The better systems use a Conditional Access System (CAS) like Conax, Cryptoworks, Nagravision, Seca, Viaccess, NDS Videoguard... As base for video/audio encryption they also use CSA but the key changes every ~10 sec.

If the video bit-rate is lower than the required bit-rate mostly zeros are appended to the video packets before the stream gets encrypted.

The CSA-Rainbow-Table-Tool is able to create a large database called Rainbow Table (RBT) [3] based of these encrypted null packets which will take a long time.

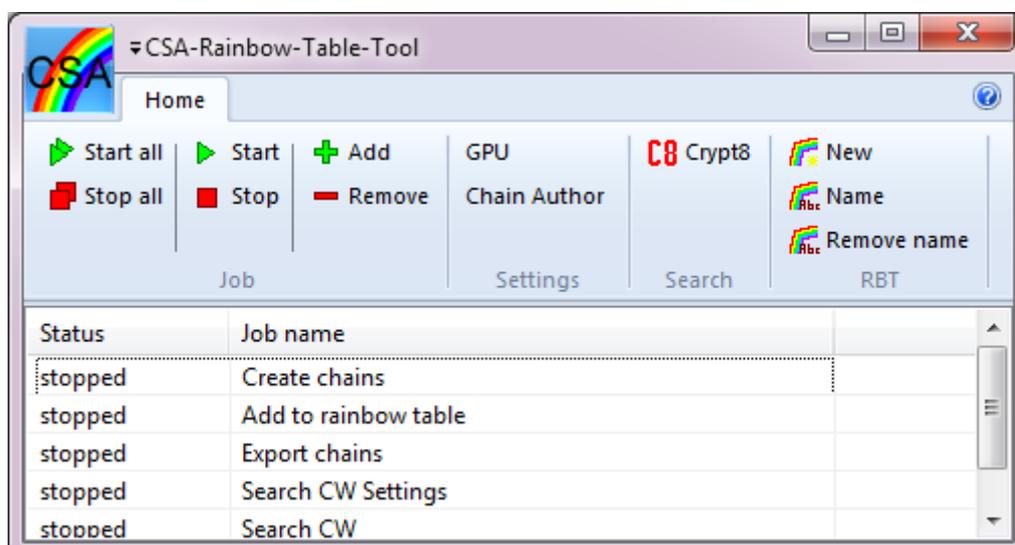
After the one time RBT creation was done it can be used for many key look-ups that are very fast.

To speedup the things the tool will use the Graphics Processing Unit (GPU) on a video card from Nvidia [2] to do the calculations necessary to create the RBT and also for the little post calculation during key look-ups.

The version 1 of the tool was fast enough to break static BISS keys, but to slow for CAS systems. On HDD a key search takes nearly one hour and on SSD only some minutes on a RBT size of 200-300 MB. The success rate is ~99%.

The version 2 was rewritten from base and the top design goal was speed.

It is able to do a key search in ~4 seconds on SSD (on HDD it takes 29 seconds). It requires 1.25 TB and the success rate is currently 77.4%. The fixed RBT size of 1.25 TB is still not full. If the community creates more chains and share it to others the success rate can be increased to maybe 90%. I don't know what success-rate a full RBT will have.



Index

Introduction.....	1
Changes between version 1 and 2.....	3
RBT.....	3
Chains are incompatible.....	3
Chain length.....	3
Chain file.....	3
Community.....	4
RBT and GPU on same or different computers.....	4
Quick start guide.....	5
GPU connection.....	5
RBT creation.....	7
Add jobs.....	8
Add chain files to the RBT.....	9
Define search settings.....	10
Search keys.....	11
Create chains and share it.....	12
Crypt8 search.....	14
Getting performance data and success rate.....	15
Special functions.....	16
Remove name.....	16
Name.....	17
References.....	18

Changes between version 1 and 2

There are many changes in version 2. The most are required to get the high speed in key look-up.

RBT

In version 1 the RBT has a variable size. When adding the first chain the size is very small. Each time a chain was added it was merged with the RBT and sorted and the complete resulting RBT was written to disk. A look-up for an end-value-prefix needs multiple read accesses (binary search). For 99% success rate it required only a few hundred MB which fits on a single SSD.

In version 2 the RBT has a fixed size of 1.25 TB even when only a single chain was added. The fixed size was necessary to speed up the look-up. A look-up for an end-value-prefix needs only one read access. Because 1.25 TB don't fit on a single SSD the tool offers an option to split the RBT to more smaller files that are located on different SSD drives at RBT creation time.

Chains are incompatible

To get the very high key search speed it was necessary to use an other chain length (1000h instead of 10000h), so version 2 can't use chains that were created with version 1.

Chain length

In version 1 a single chain contains 10000h values. So with the storage of 12 bytes (6 byte start value and a 6 byte end value of that chain) 10000h keys can be found, but post calculation after a look-up takes very long.

In version 2 a single chain contains 1000h values. So with 12 bytes only 1000h keys can be found, but post calculation after a look-up is much faster.

There are good and half-good chains. At creation time they can't be identified.

In version 1 all chains get added to the RBT.

In version 2 only good chains will be added to the RBT. Half-good chains will not be added. This makes the post calculation faster.

If an end-value is already present in the RBT but the start-value is different, than it is a half-good chain, because only from the start-value to ca. the middle of the chain it contain new keys, but from the middle to the end-value the keys are already present in the RBT.

Chain file

The speed to create x keys per second is the same in both versions. But because the chain length in version 2 is 10h times shorter, the creation time for a chain file is also 10h times faster. Of course we need much more chain files to find the same amount of keys. Also not adding half-good chains and only good chains from a chain file to the RBT increases the need of much more chains.

Community

In version 1 chain sharing was not needed. But in version 2 we need so many chains that for a single person it's not practicable (I needed more than a year to get 77.4% success rate and the RBT has still space for more chains available). In the new version anyone can create chains and add it to the RBT, but the key search will only use chains that are listed in a small (non text) file called ChainAuthor.map. If you have created a chain file and share the download link to our community than I will add the chain file name to the ChainAuthor.map file and upload it regularly. But it's not required to create own chains, for the case you have only a slow speed GPU card. You can download my chain files that I have already created (which I try to upload as fast as possible and also an up-to-date ChainAuthor.map – check my homepage [1] for info) to reach 77.4% success rate.

RBT and GPU on same or different computers

The tool requires that the RBT is on the same computer and in version 1 the GPU also. In version 2 the GPU can still be on the same computer, but it can access one or more GPUs on other computers also.

The new version has the following two exe files:



CSA-Rainbow-Table-Tool.exe (the main application that is running on the computer where the RBT file is stored)



CSA_CUDA_Server.exe (the agent that is running on the computer with the GPU card(s) that you want use)

In the tool you can define one or more computers that has the CSA_CUDA_Server.exe running.

Quick start guide

If you want only to use the basic features in a simple setup you can use this short guide.

- You are using the tool, RBT, and GPU on a single computer
- You have already crypt8 values (of encrypted “NULL packets” = plain type B8hx00h) and you want know the keys.

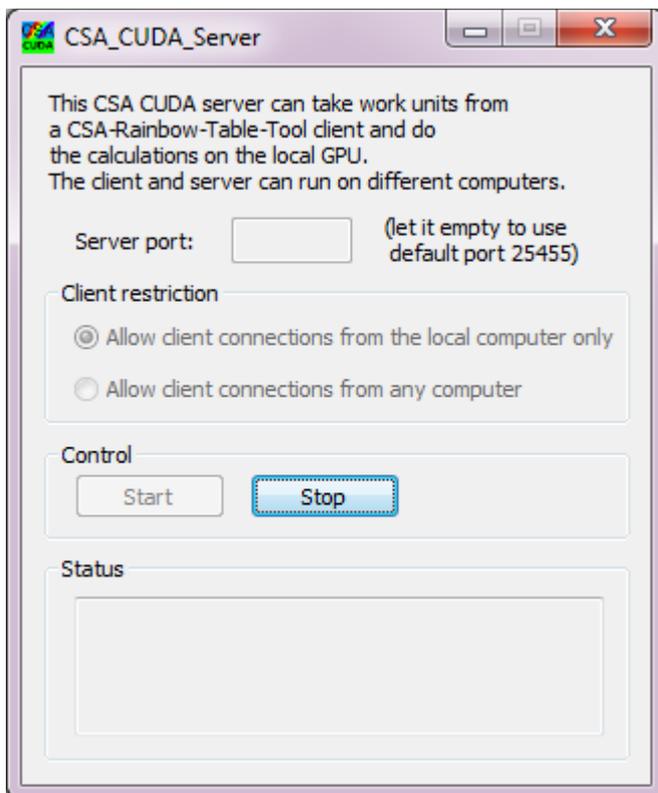
GPU connection

Run the CSA_CUDA_Server.exe

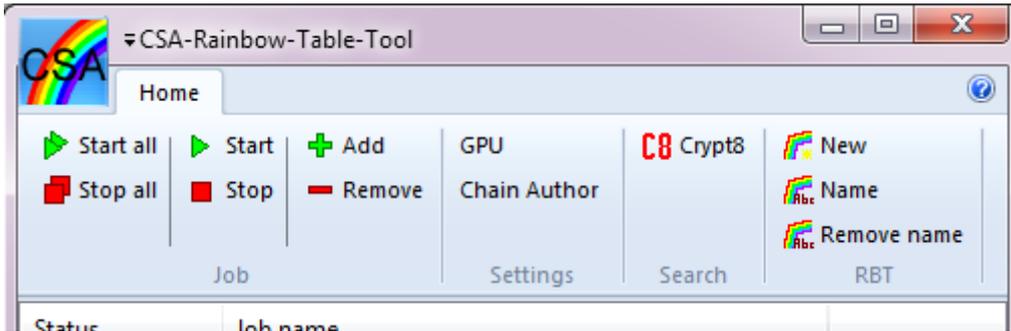
Select “Allow client connections from the local computer only” and click “Start”

Maybe the Windows firewall is asking for permission now.

If you run the CSA_CUDA_Server.exe the next time it will start automatically with these settings.



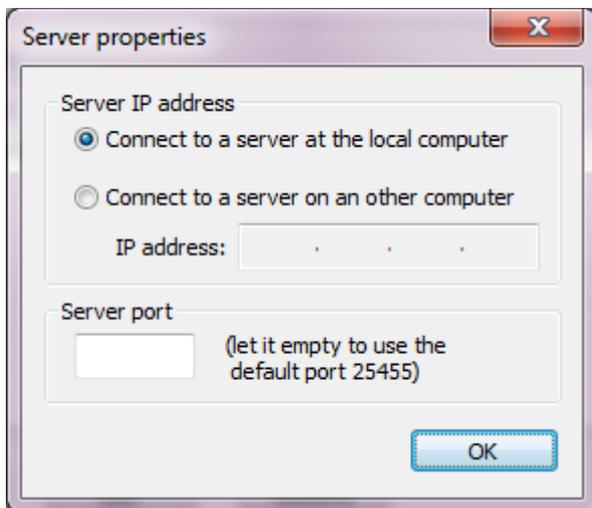
Run the CSA-Rainbow-Table-Tool.exe



Click "GPU" in the settings menu

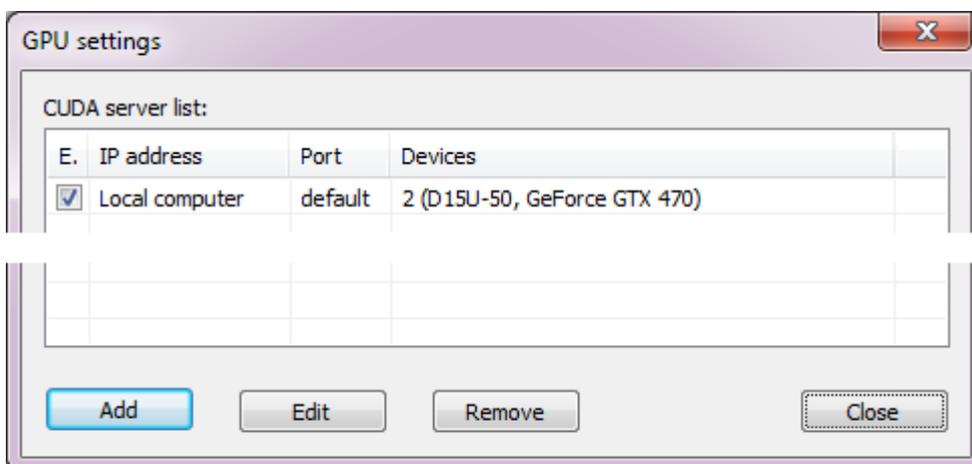
Click "Add" inside the GPU settings dialog

Select "Connect to a server at the local computer" and click "OK"



Now the tool will connect to the CSA_CUDA_Server and retrieve and show a list of available Nvidia GPUs. At least one device must be shown to successfully continue.

Click "Close"



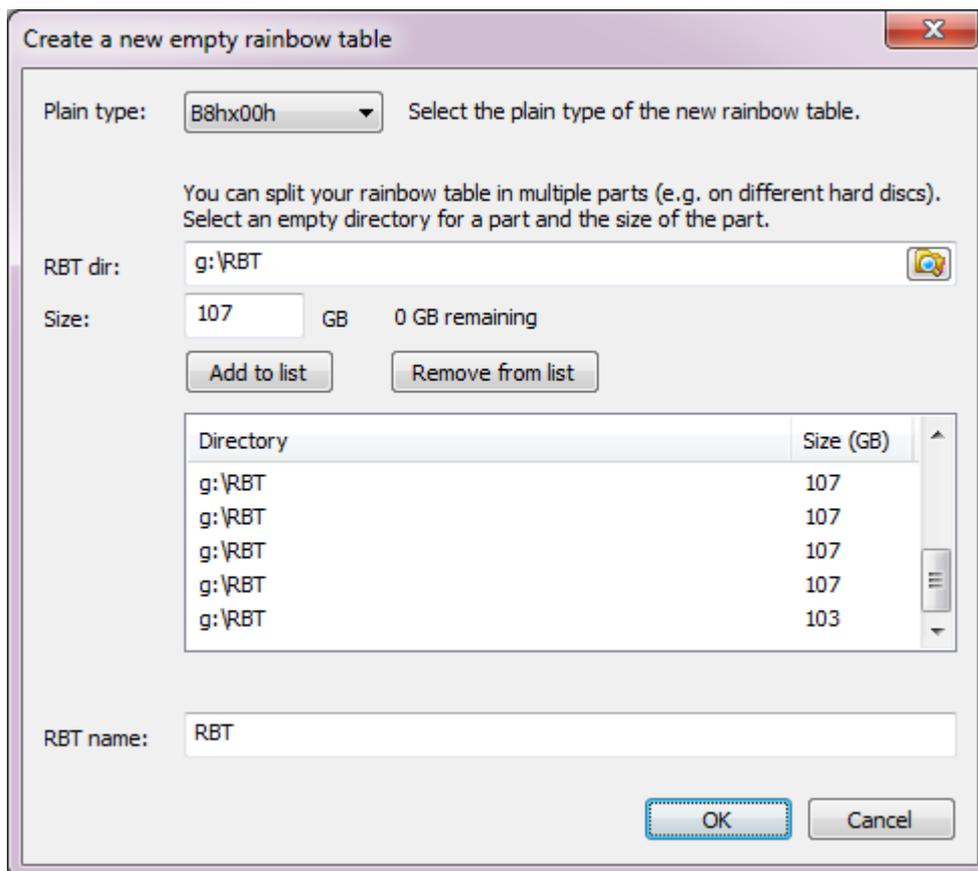
Go to my homepage [1] and check where you can find the file ChainAuthor.map and download it

Click “Chain Author” in the settings menu

In the “Chain Author map” dialog enter the location of the ChainAuthor.map file and click “OK”

RBT creation

To create an empty RBT click “New” in the RBT menu



Select plain type “B8x00h”

Now you can split the RBT to multiple files. After creation the size of each file can't be changed anymore.

A single file of 1280 GB will may be fit on your 2 TB HDD. But will prevent you to move it to two 1 TB SSD later when SSD becomes cheaper.

But creating more than 20 small files will maybe has a negative effect to the RBT performance.

I have decided to use 12 files for my RBT.

In the windows explorer create a RBT directory that you want to use and enter it in the field “RBT dir”

As size enter 107 and click 11 times “Add to list”

As size enter 103 and click one time “Add to list”

Enter a RBT name e.g. “RBT”

Click “OK” and the files will be created very fast.

Add jobs

Add three jobs that we need later:

Click “Add” in the Job menu

select “Add to rainbow table” and click “OK”

Click “Add” in the Job menu

select “Search CW Settings” and click “OK”

Click “Add” in the Job menu

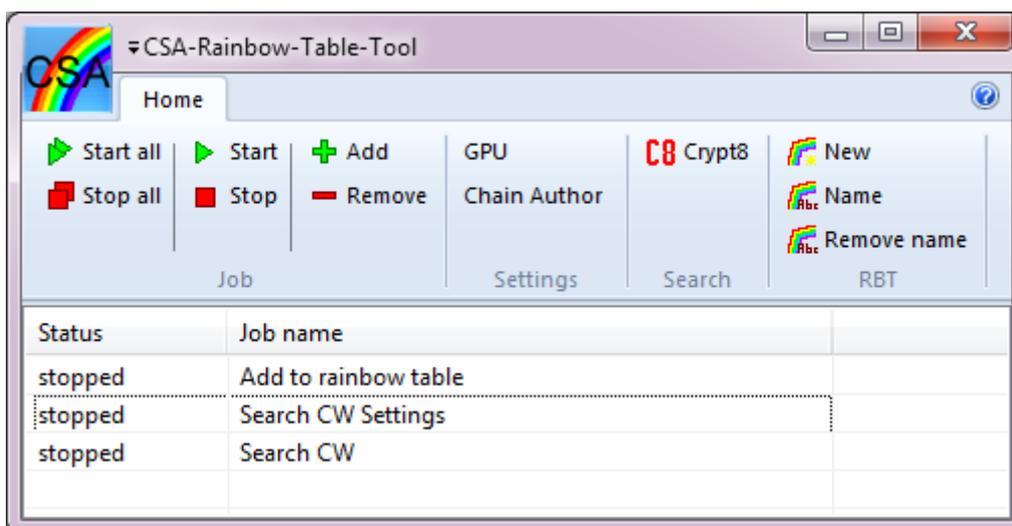
select “Search CW” and click “OK”

The tool remembers the jobs when you close and reopen it.

When adding a new job the job settings dialog will also be shown. If you have closed it you can reopen it anytime via a double click on the job name in the main window of the tool.

Closing a job settings dialog doesn't stop a running job. Only pressing the “stop” button or closing the tool will stop the job.

You can also start and stop a selected job in the main window or use start all/stop all.



Add chain files to the RBT

Before we can find a key we must add chain files to the rainbow table.

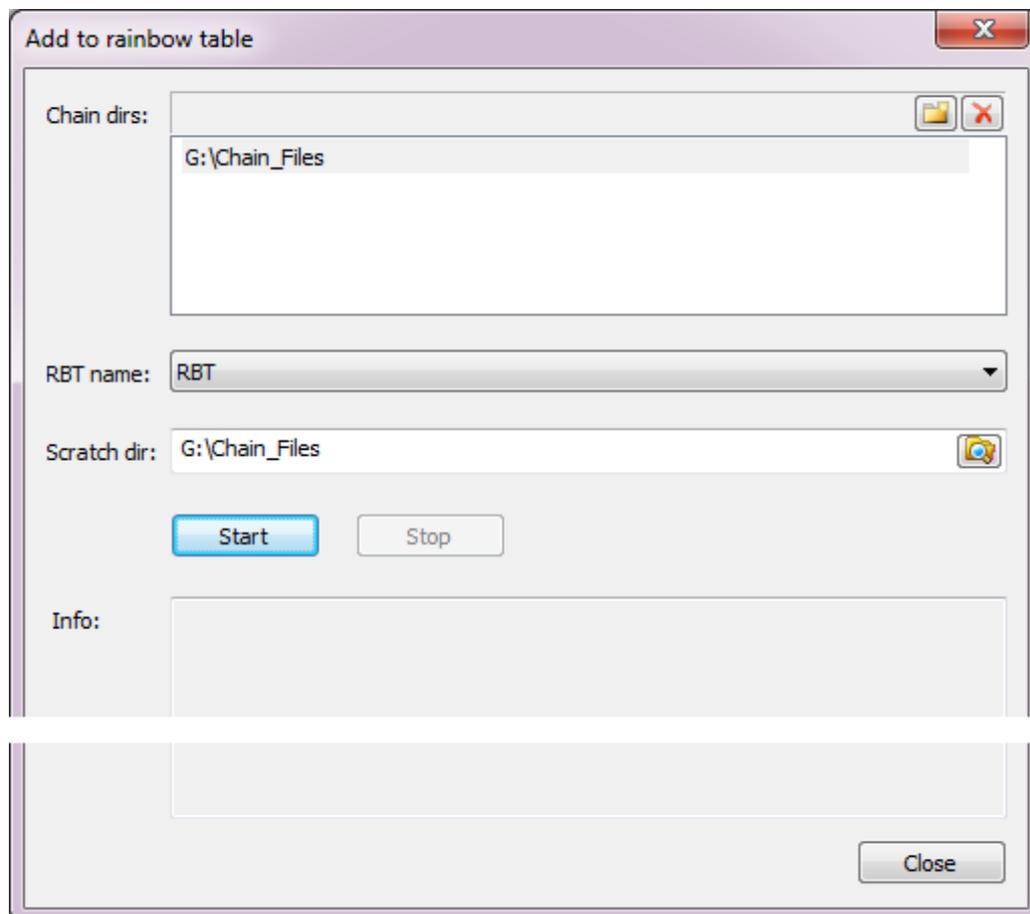
Check my homepage [1] where you can find my chain files that I have created already and download them.

Click on the yellow folder icon and add the directory where you have stored the downloaded chain files (don't forget to unpack it).

Select the name of your RBT

Create an empty folder via the windows explorer and select it as scratch directory. It will be used as temporary directory to split, sort, and merge chain files. It must have enough free hard disk space.

Click "Start" to merge it to your RBT. This can take a long time.



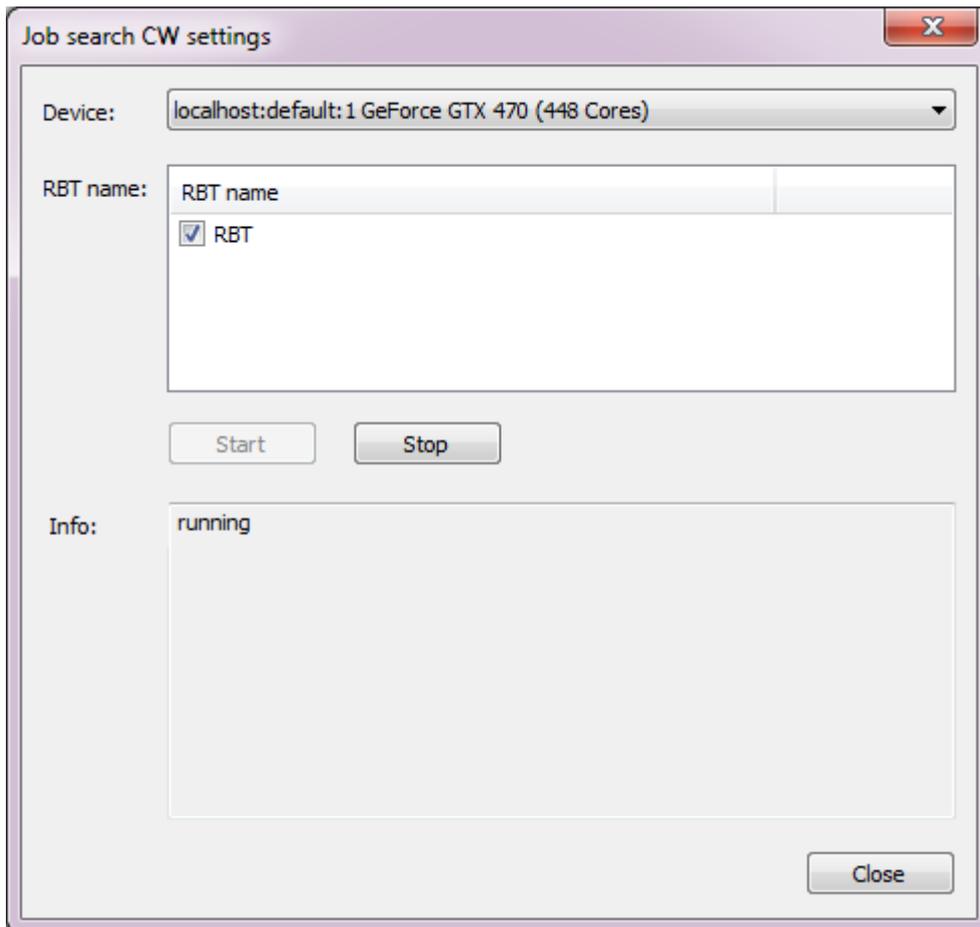
Define search settings

After you have merged all chain files double click “Search CW Settings” to change the settings.

Select a GPU device that you want to use for the key search

Enable the check-box near your RBT name that you want use

Click “Start” and close the dialog



Search keys

Double click "Search CW" in the main window of the tool

Enter or copy one or more Crypt8 values to the input box

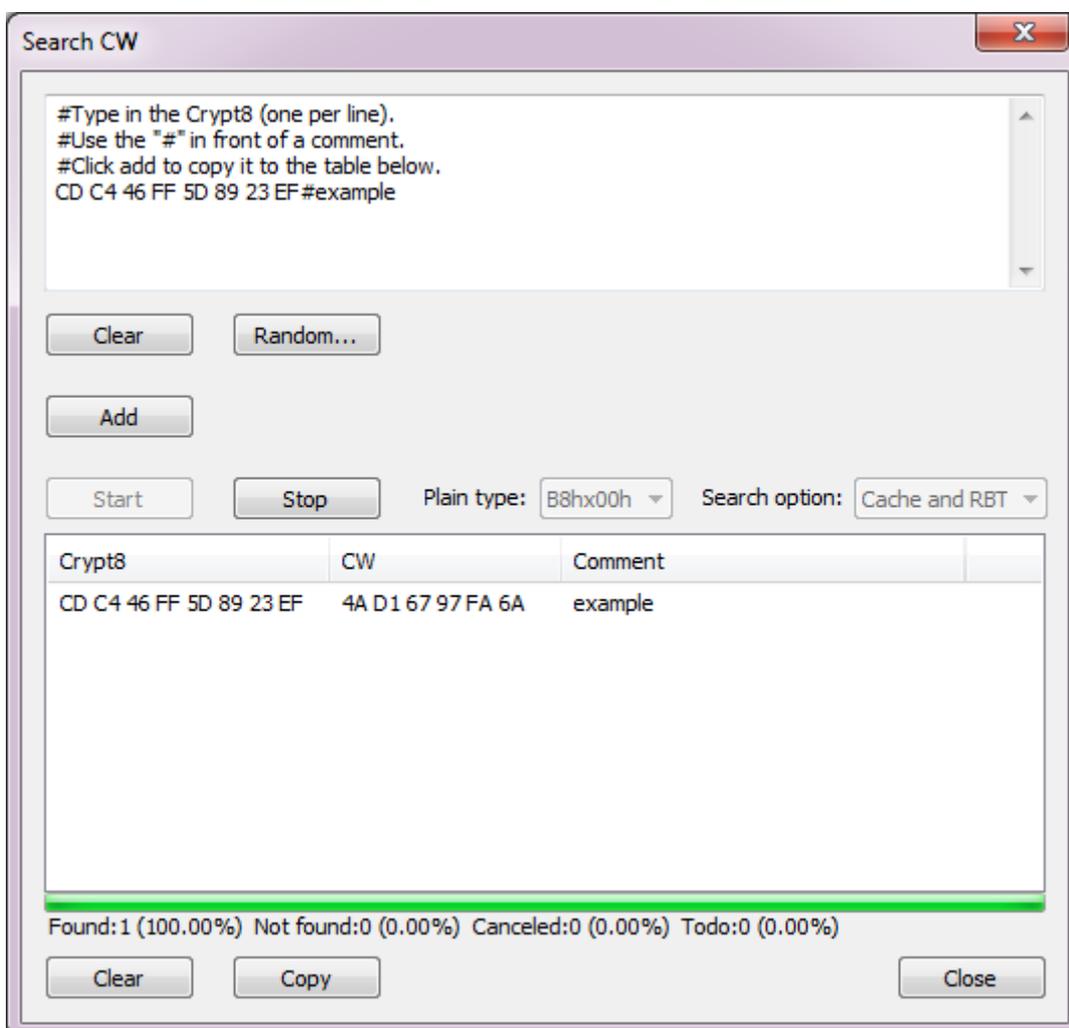
click "Add" to copy it to the list below

select "B8hx00h" as plain type

select "Cache and RBT" as search option

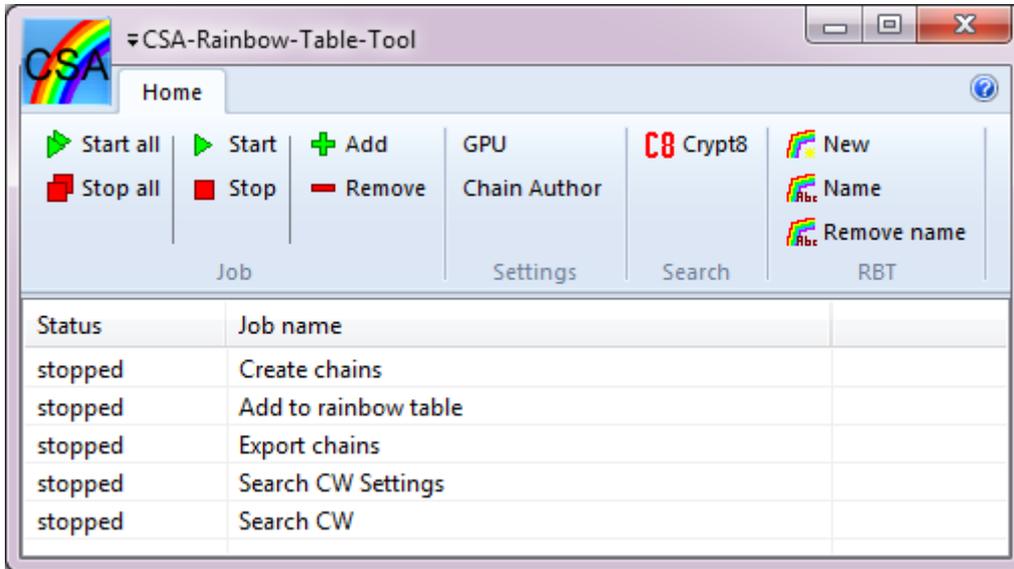
click "Start"

After the key search has finished you can copy the results by clicking the "copy" button.



Create chains and share it

To create chains click “Add” in the job menu select “Create chains” and click OK

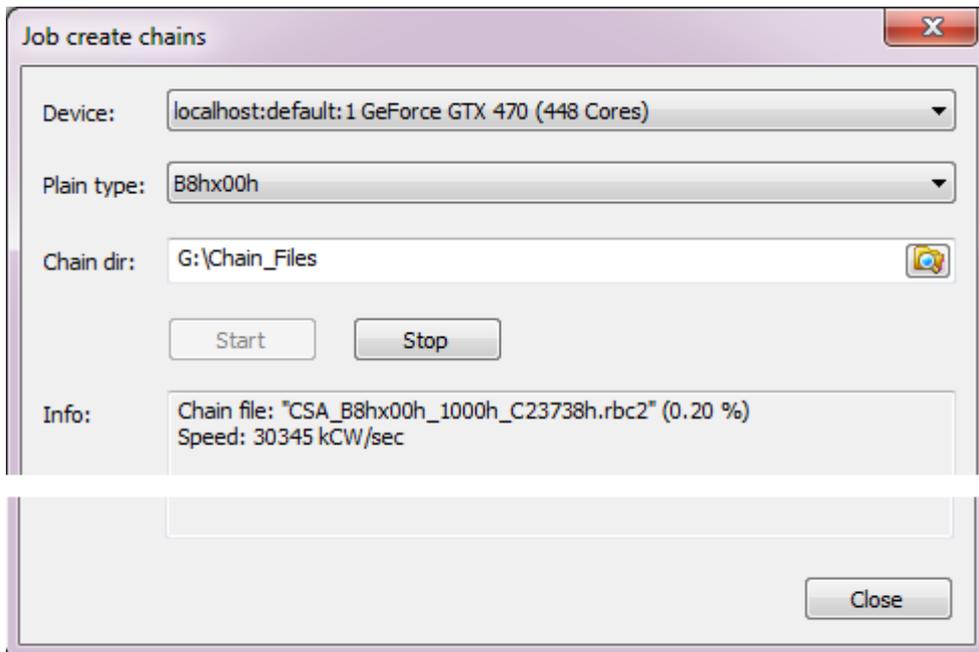


select the device you want to use to create chain files

select the plain type “B8hx00h”

Enter a directory where the chain files will be saved

Click “Start”



After you have enough chain files with file extension “.rbc2” don't share it directly.

A “.rbc2” file has a fixed size of 384 MB and because the community has already many chains present in their RBT only a small part of the 384 MB will be added to their RBT. So you waste your upload bandwidth and the download bandwidth of all members of our community if you upload “.rbc2” files. I don't plan to include such chain names to the required “ChainAuthor.map” file.

It's better to upload only the small needed part of an “.rbc2” chain file. This smaller chain file has the extension “.rbc3”.

How to convert a “.rbc2” to a high efficient “.rbc3” chain file?

First ensure that you have added all chains shared by the community to your own RBT.

Then get the newest “ChainAuthor.map” and select it in the tool.

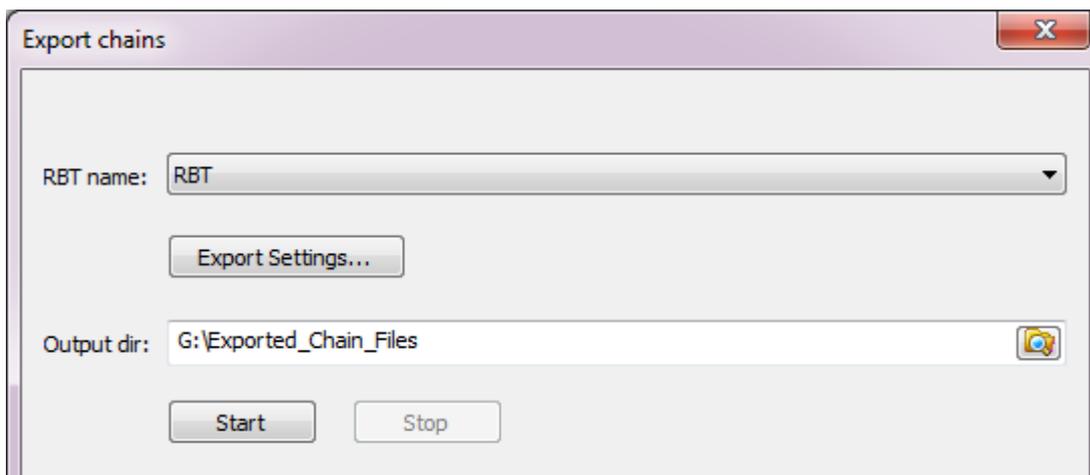
Then add all your own created chains to your RBT.

Add a new job called “Export chains”

Select the name of your RBT

Enter an output directory for the exported chains

Click “Export Settings...”



In the export settings dialog click “Read part of RBT”

Then you will get a list of start-values.

To not confusing the user by a very large list with all start-values contained in the RBT and the user must select the own ones for export I have made it easier.

The list will hide all start-values that the community already has and an export isn't needed (all chains listed in the “ChainAuthor.map” will be hidden).

So the list contains mainly your own chains. So the selection which chain files you want export and not export is easier.

Because only a part of the RBT was read not all your chains may be on the list, but if the tool will find a chain during export that was not shown on the list it will also export this chain.

After you have made your decision close the export settings dialog and click “Start”.

The export will takes a long time because the full RBT must be read, and chains must be collected and sorted. The time will be more or less the same for exporting only one or many chains. So it's to time consuming for only exporting a few chains.

Don't upload each small “.rbc3” file separately. Add multiple small “.rbc3” files to a rar/zip file and upload it.

Check my homepage [1] for the information where to post the links to get listed in the ChainAuthor.map.

Crypt8 search

To extract crypt8 values from a Transport Stream (TS) file click “Crypt8” in the search menu.

Enter the TS file name

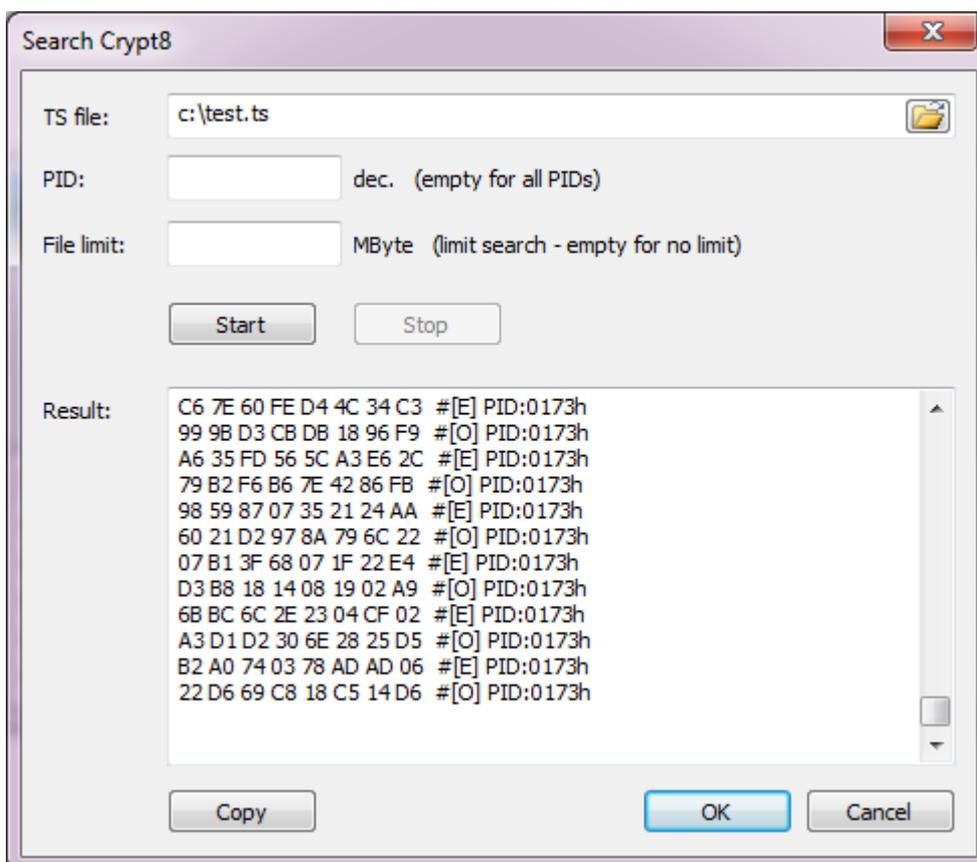
Optionally you can limit the search to a specific PID.

Optionally you can search only a part of a TS file.

Click “Start”

Click “Copy” to copy the results

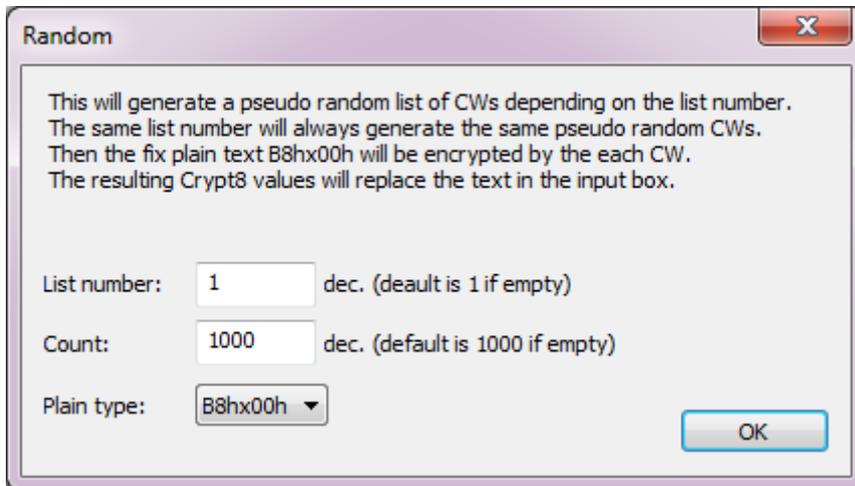
After that you can insert the crypt8 values to the search CW dialog to find the corresponding keys.



Because the crypt8 values are encrypted the tool can't recognize if they are encrypted B8hx00h or e.g. B8hxFFh filling packets.

Getting performance data and success rate

Open the “Search CW” Job and click the “Random...” button



Enter the list number 1

Enter the Count 1000

Select the plain type “B8hx00h”

Click OK

Select the search option “RBT only” to prevent cache look-ups

Select plain type B8hx00h

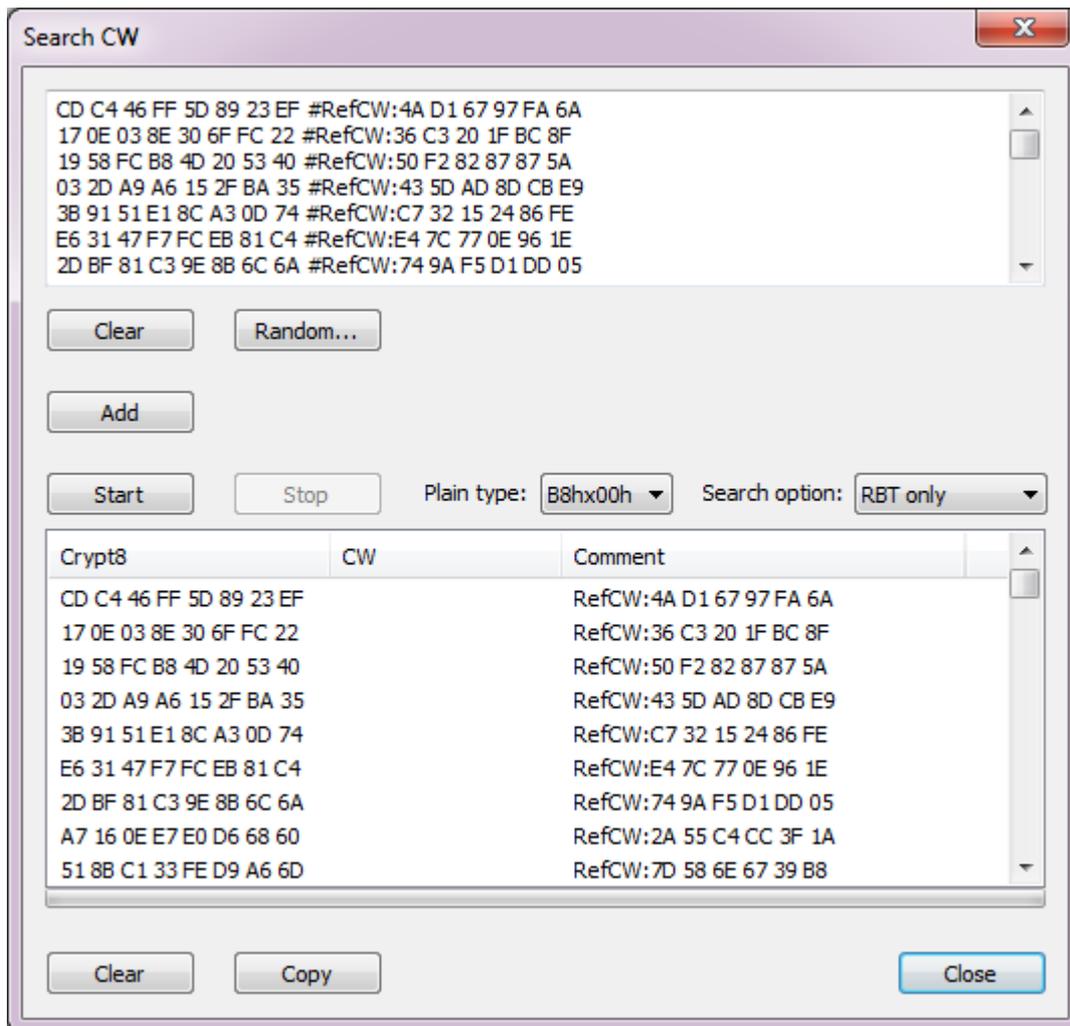
Click “Add”

Click “Start”

Stop the time till the search of the 1000 keys has finished. Divide the time to 1000 and you have the seconds per key value.

If you are only interested in the success rate than use the search option “Cache and RBT”. Every found CW will be stored in a cache file. If you run it again (e.g. after you have added more chains to your RBT – don't forget to update the “ChainAuthor.map”) than the every key found in the cache don't need a RBT look-up and post processing. So it's faster to get the success-rate.

After the search the tool will show the percent of found CWs. It should be at least 77.4% if you have added all my chain files.



Special functions

The following functions in the RBT menu are normally not needed.

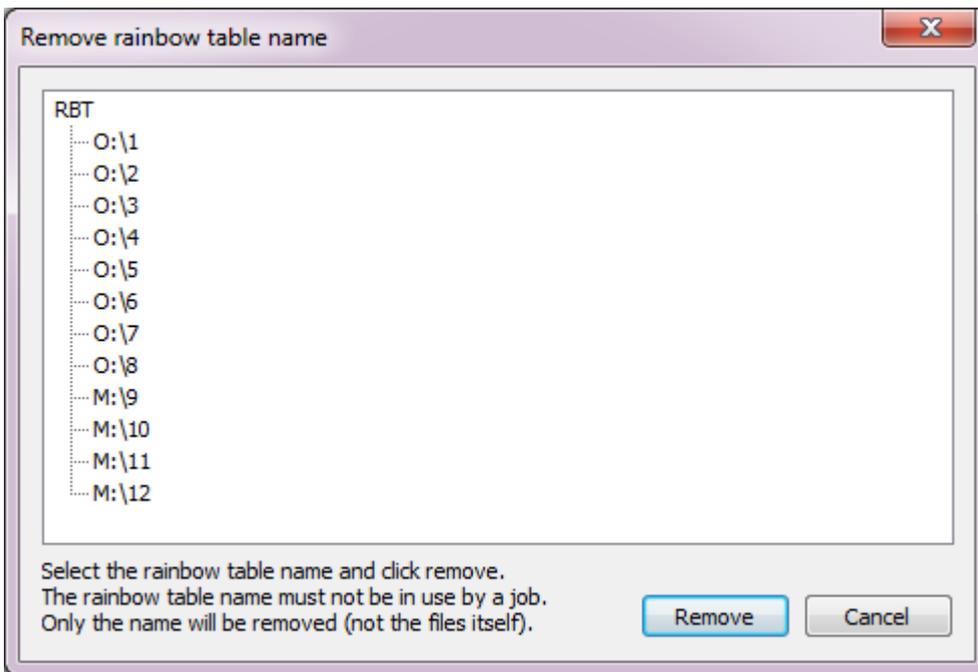
“Remove name” and “Name”

Remove name

To remove your RBT name from the tool (not the files itself) click “Remove name” in the RBT menu

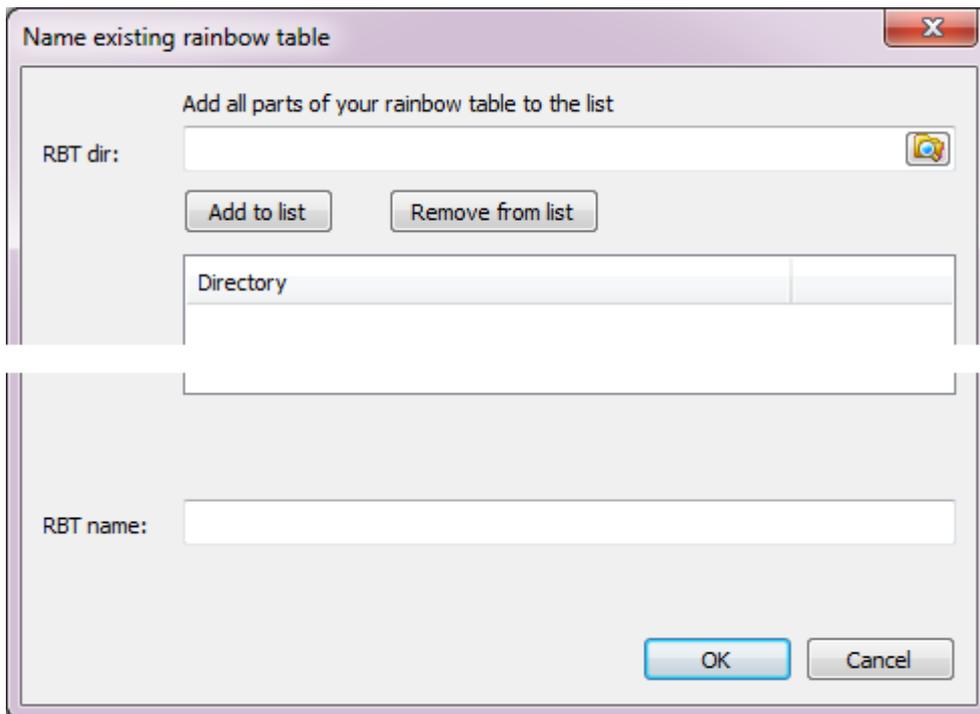
Select the RBT name (e.g. “RBT” in the example below)

Click Remove



Name

If you have lost your “CSA-Rainbow-Table-Tool.ini” but have still your RBT files then click “Name” in the RBT menu.



Enter the directory where a part of your RBT file is located to the “RBT dir” field and click “Add to list”

Repeat it till all parts are in the list

Enter a name that you want give your RBT in the “RBT name” field and click “OK”.

References

[1] At the authors homepage <http://colibri-dvb.info> you will find the up-to-date tool and documentation. Also the information where you get the chain files and the ChainAuthor.map file. There's also a forum link on the homepage.

[2] You need a graphic card from <http://www.nvidia.com> with CUDA support and drivers to use this tool.

[3] https://en.wikipedia.org/wiki/Rainbow_table