

SMR-F Container Tool

Binary extraction from SMR-F containers · BinRazor

What it does

An SMR-F file is an encrypted flash container used for control-unit firmware. The firmware inside is not stored in plain form — it is encrypted. This tool opens such a container, reads its metadata, and extracts the firmware as a decrypted, plain binary (.bin) file you can view, edit or analyse in other tools.

About the container

Beyond the raw firmware, an SMR-F header carries descriptive information about the flash: when it was built, its revision, the ODX version and the compiler used. The tool reads this automatically so you can confirm you are working with the right file before extracting anything.

Step 1 — Open the container

Click Open and choose your .smr-f file. The tool reads the container and fills the log panel with the metadata it found:

Date / Time	When the flash file was created.
Revision Info	The revision identifier of the firmware.
ODX Version	The ODX data version used.
Trafo Compiler	The compiler/version that produced the container.
Segment Size	The size of the firmware segment, in bytes (also shown in hex).

Step 2 — Extract to .bin

With a container open, click Export. The tool locates the firmware inside the container, decrypts it, and asks where to save the result. It writes the decrypted firmware as a new .bin file, named after the source container by default.

What happens during extraction

The firmware in an SMR-F is stored encrypted. During Export the tool finds where the firmware segment begins (from the size recorded in the header), reads it to the end of the file, and decrypts every byte to reconstruct the original firmware. The container itself is never modified — you always get a fresh copy.

The output file

The result is a plain, decrypted binary containing the firmware only — no SMR-F header or encryption around it. It is ready to be opened in a hex editor, compared, or processed by the other BinRazor tools.

Good to know. Export is a read-only operation: it never alters the source container, so it is completely safe to open a file and extract its firmware. The tool works specifically with .smr-f containers.