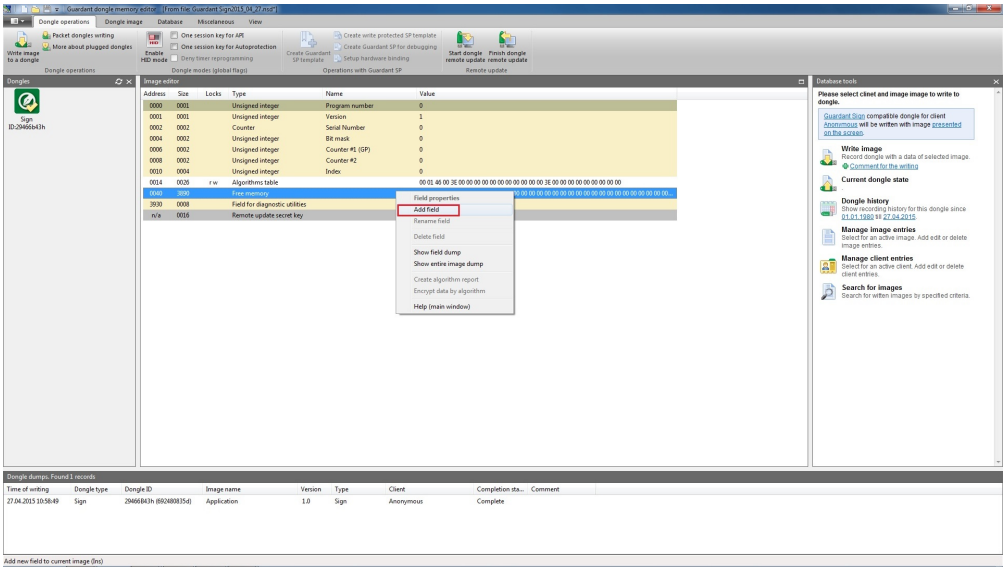
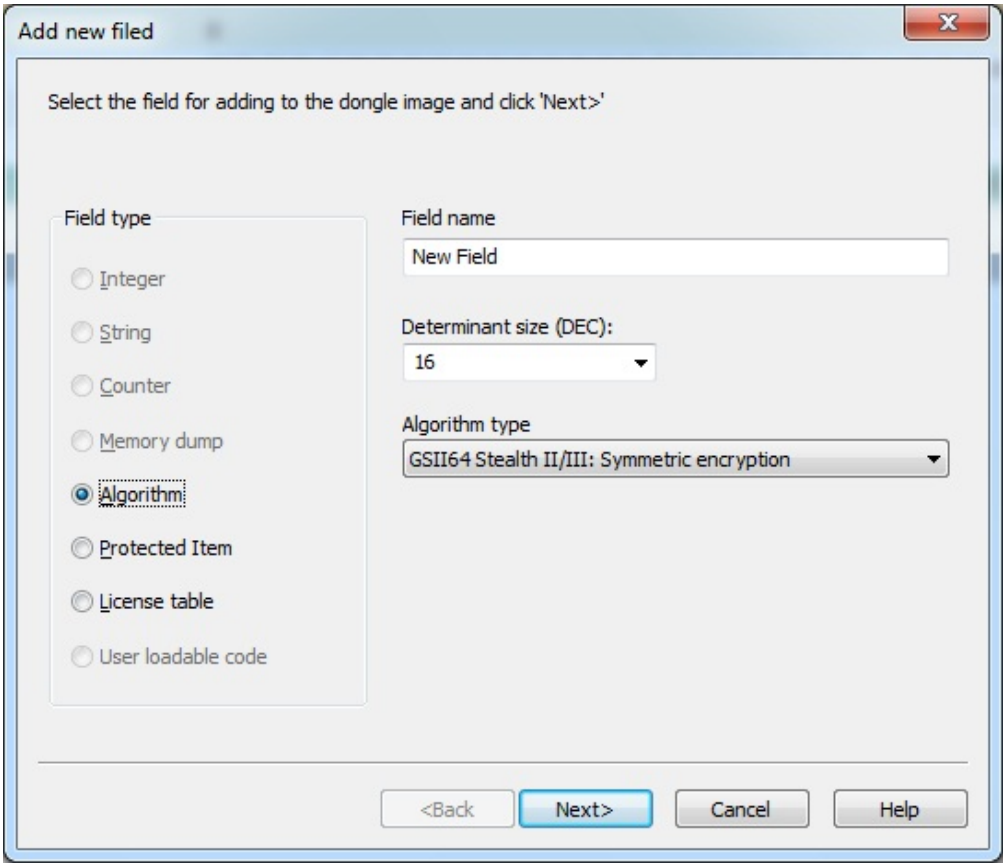
Creating Algorithm

To create a hardware algorithm execute command **Edit | Add field**.

In **Add field** dialog box that will appear select **Algorithm** field type, specify the name and the type of the new algorithm as well as the size of its determinant.

Add new algorithm dialog box:





Algorithm type

Select an algorithm type from the dropdown list.

The type of algorithm being created depends on the dongle mask:

Mask type	Algorithm type
Guardant Time/ Time Net Guardant Sign/ Sign Net	1. Symmetric encryption: GSII64 2. Symmetric encryption: AES128 3. Digital signature generation: ECC160 4. Hash function generation: HASH64 5. Hash function generation: SHA256 6. Random numbers generation: RND64
Guardant Code/ Code Time	1. Symmetric encryption: AES128 2. Digital signature generation: ECC160 3. Hash function generation: SHA256
Guardant Stealth III / Net III	1. Symmetric encryption: GSII64 2. Hash function generation: HASH64 3. Random numbers generation: RND64
Guardant Stealth II / Net II	1. Symmetric encryption: GSII64 2. Unidirectional algorithm Stealth I and its modifications: Fast, Random, AutoProtect
Guardant Stealth / Net	Unidirectional algorithm Stealth I and its modifications: Fast, Random, AutoProtect
Guardant Fidus	-

Size of determinant

Determinant – the main part of hardware algorithm descriptor, which defines the specific type of encryption function. Algorithm determinants in Guardant dongles have fixed even length, Using GrdUtil.exe you can set the size of determinant and edit its type.

In order to select (or set – for unidirectional algorithm Stealth) the size of determinant, use the combined field-list.

The size of determinant depends on the algorithm type:

Algorithm type	Size of determinant, bytes
Symmetric encryption: AES128	16
Digital signature generation: ECC160	20
Symmetric encryption: GSII64	16 or 32
Hash function generation: SHA256	-
Hash function generation: HASH64	16 or 32
Random numbers generation: RND64	16 or 32
Unidirectional algorithm Stealth I – obsolete	4 – 200 (optimum - 32)

After setting the type and size of determinant of a new algorithm you need to edit its properties. Click **[Next]** in the lower part of the dialog box to move to the next page.