How to use Emsisoft Decryptor to recover files encrypted by DJVU ransomware

For all versions of STOP Djvu, the information can be decoded correctly, if they are encrypted using an offline key available to the developers of Emsisoft Decryptor.

There are certain restrictions regarding which files can be recovered. Talking about all versions of STOP Djvu, the information can be decoded correctly, if they are encrypted using an offline key available to the Emsisoft Decryptor developers.

For Old Djvu, files can also be decoded with original / encrypted file pairs, provided to the STOP Djvu portal. These are identical files (because they contain the same data), except for an encrypted copy, and the other is not.

The STOP Djvu portal can analyze the difference between an encrypted file and an original of the same file, allowing it to determine how to decode the file. For most victims who have an older version of STOP / Djvu, sending file pairs is the only way for them to get their files back.

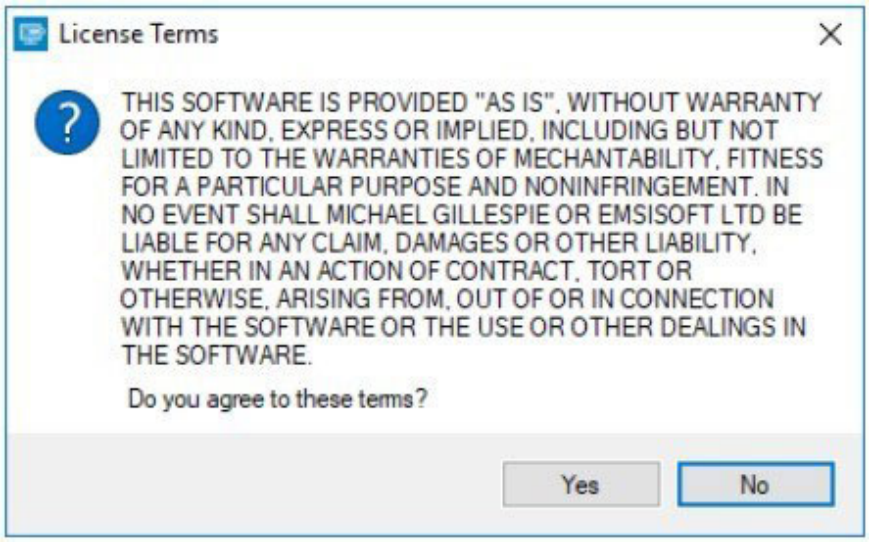
Remember that this does not apply to New Djvu built after August 2019.

How to recover your files?

1. Start by downloading the STOP Djvu decoding tool.

https://www.emsisoft.com/ransomware-decryption-tools/download/stop-djvu

2. Make sure to start the decryption utility with admin rights. You need to agree to the license terms given, by clicking the **Yes** button **.**

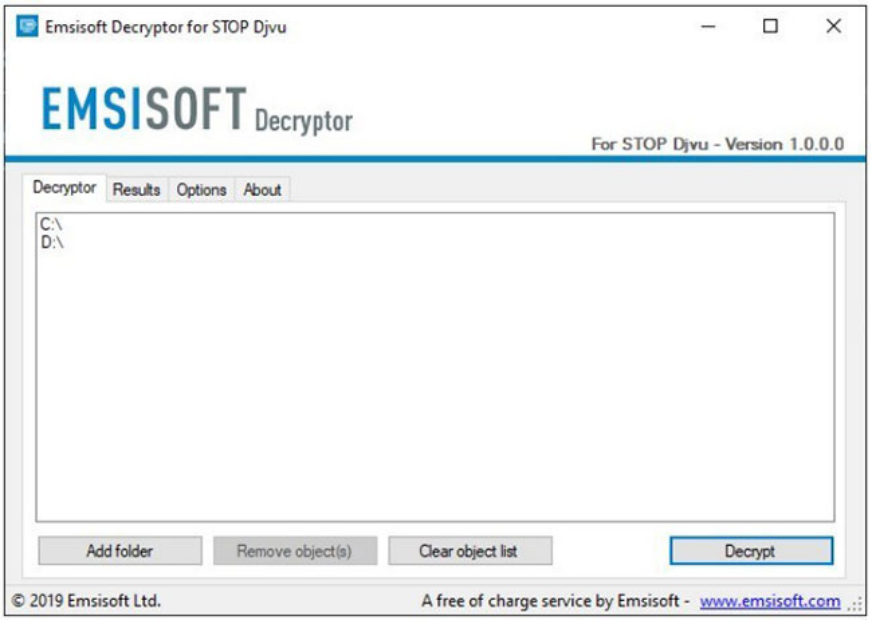


You need to agree to the license terms given
3. As soon as you accept the license terms, the main Emsisoft Decryptor user interface will appear.

4. Based on the default settings, the decoder will automatically fill in available locations to decode existing drives (connected drives), including network drives. You can choose additional locations (optional) with the help of the **Add** button **.**

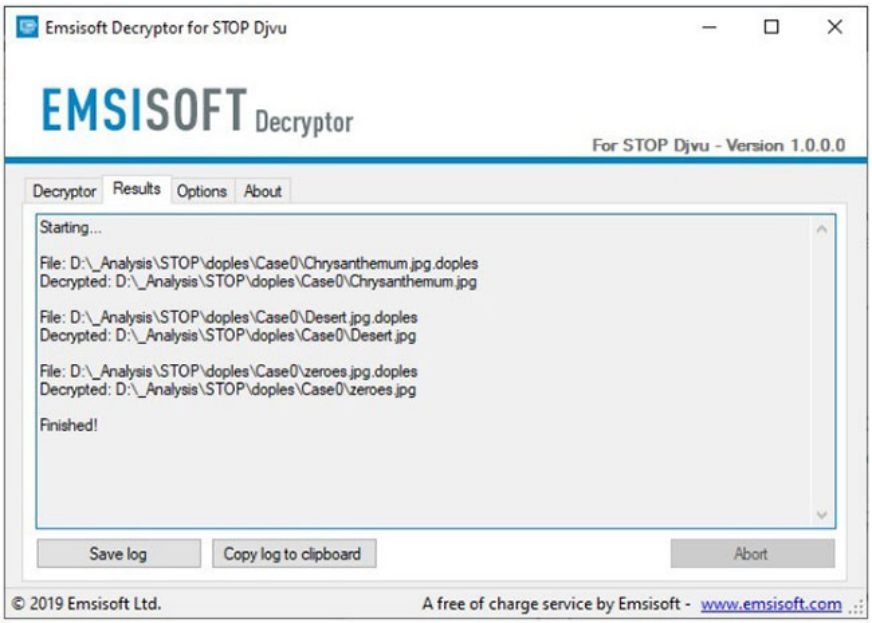
5. Decoders often suggest a number of options considering specific malware families. The options can now be displayed in the **Options** tab and can be activated or deactivated there. You can define a detailed list of currently active options below.

6. As soon as you add all the desired locations to decrypt to the list, click the **Decrypt** button to start the decryption process. Note that the main screen can switch you to the status view, telling you the operating procedure and the decoding statistics for your data.



Click the Decrypt button to start the decryption process

7. The decoder will notify you as soon as the decoding process is complete. If you need to report a personal document, you can save it by selecting the **Save log** button **.**



Click the Save log button to save the report
Note that it is also possible to copy the report directly to the clipboard and paste it into email or forum messages if needed.

Decoding options for DJVU

The decoder at this time provides the option to keep the encrypted files

Considering the fact that ransomware does not store any data related to unencrypted documents, the decoder does not guarantee that the decrypted file will be identical to the original encrypted data. Therefore, the decoder, based on default settings, for safety reasons will not delete any encrypted documents after they are decoded.

In case you want the decoder to delete any encrypted documents after decoding, you can turn off this feature. Note that this option can be applied if space on your hard drive is limited.