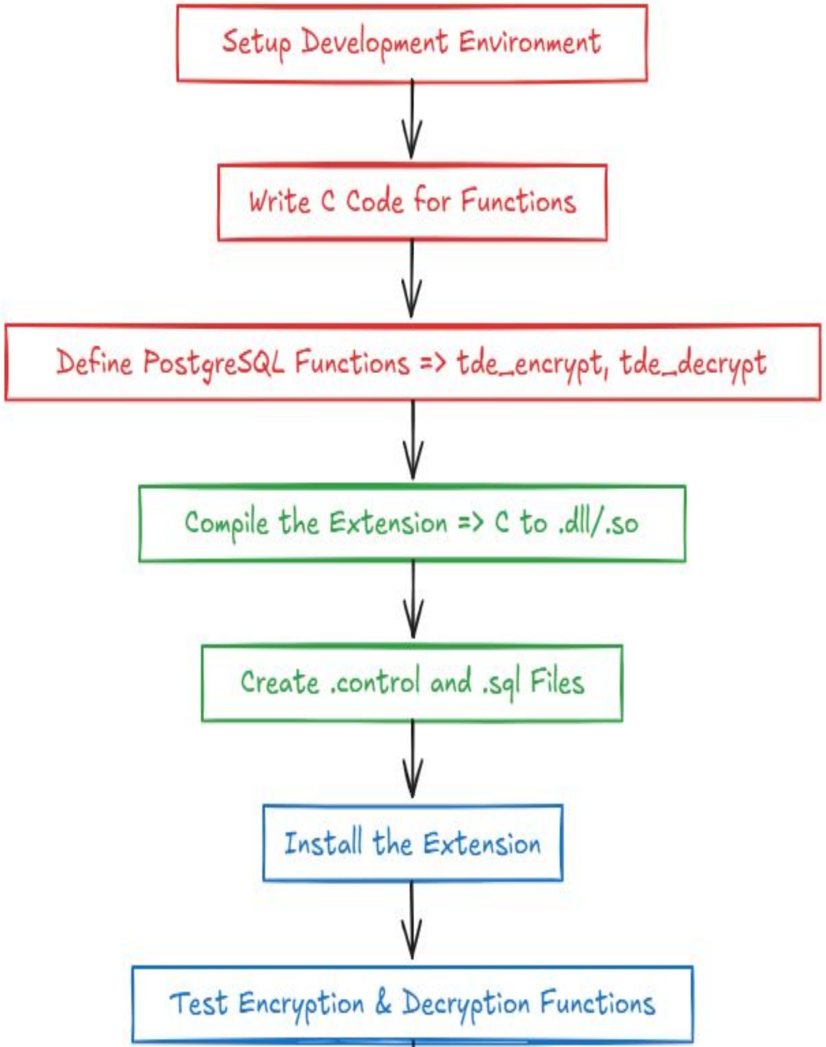
Simple Custom TDE Extension

Musab Khan

Github https://github.com/musabaku/custom-tde-extension/blob/main/tde_extension.c

Workflow for Developing PostgreSQL Encryption Extension

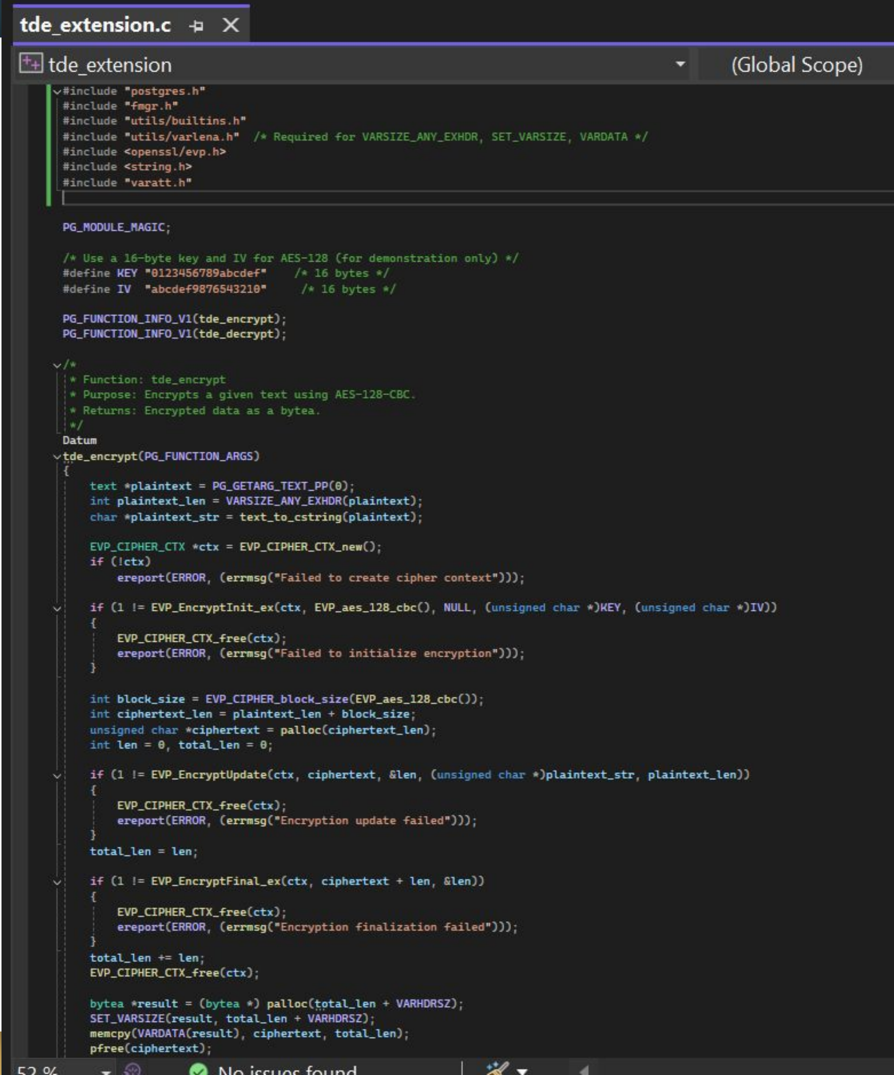
1. **Setup Environment:** Install PostgreSQL and OpenSSL. Configure Visual Studio for PostgreSQL development.
2. **Write C Code:** Implement `tde_encrypt` and `tde_decrypt` functions using OpenSSL (AES encryption).
3. **Compile Extension:** Build the C code to create `.dll` file.
4. **Create Control & SQL Files:** Define metadata in `.control` and map functions in `.sql`.
5. **Install Extension:** Copy files to PostgreSQL directories and run `CREATE EXTENSION tde_extension;`.
6. **Test Functions:** Use SQL to test `tde_encrypt` and `tde_decrypt`.


Setup Development Environment
Write C Code for Functions
Define PostgreSQL Functions => tde_encrypt, tde_decrypt
Compile the Extension => C to .dll/.so
Create .control and .sql Files
Install the Extension
Test Encryption & Decryption Functions

Tde_extension.c file

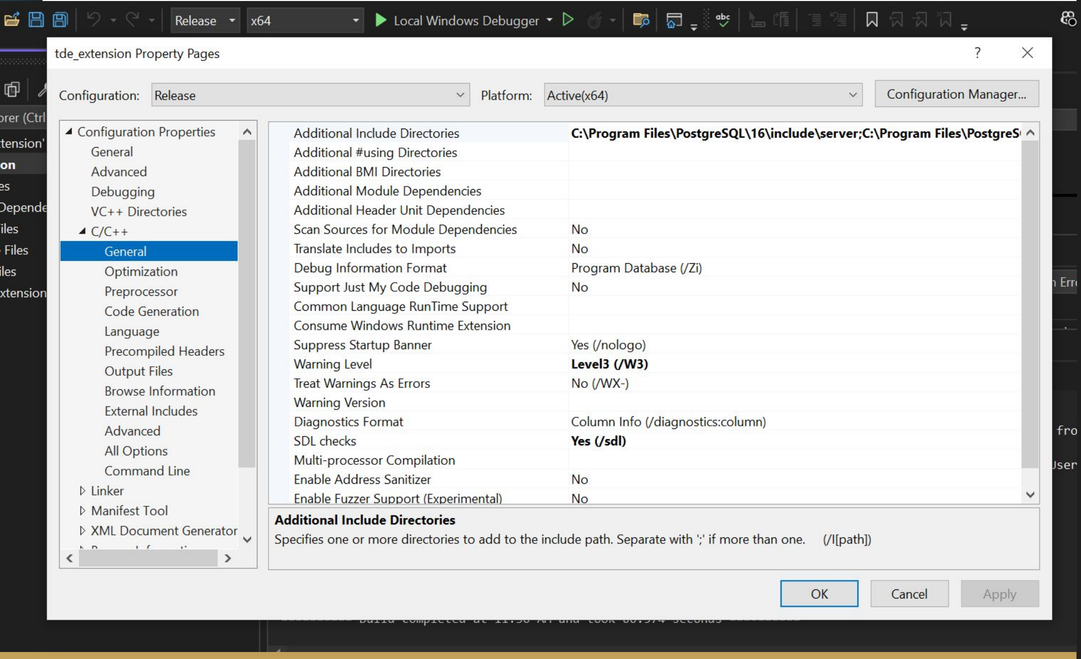
Code can be found here:

https://github.com/musabaku/custom-tde-extension/blob/main/tde_extension.c



```c
#include "postgres.h"
#include "fmgr.h"
#include "utils/builtins.h"
#include "utils/varlena.h"  /* Required for VARSIZE_ANY_EXHDR, SET_VARSIZE, VARDATA */
#include <openssl/evp.h>
#include <string.h>
#include "varatt.h"


PG_MODULE_MAGIC;

/* Use a 16-byte key and IV for AES-128 (for demonstration only) */
#define KEY "0123456789abcdef"    /* 16 bytes */
#define IV  "abcdef9876543210"     /* 16 bytes */

PG_FUNCTION_INFO_V1(tde_encrypt);
PG_FUNCTION_INFO_V1(tde_decrypt);

/*
 * Function: tde_encrypt
 * Purpose: Encrypts a given text using AES-128-CBC.
 * Returns: Encrypted data as a bytea.
 */
Datum
tde_encrypt(PG_FUNCTION_ARGS)
{
    text *plaintext = PG_GETARG_TEXT_PP(0);
    int plaintext_len = VARSIZE_ANY_EXHDR(plaintext);
    char *plaintext_str = text_to_cstring(plaintext);

    EVP_CIPHER_CTX *ctx = EVP_CIPHER_CTX_new();
    if (!ctx)
        ereport(ERROR, (errmsg("Failed to create cipher context")));

    if (1 != EVP_EncryptInit_ex(ctx, EVP_aes_128_cbc(), NULL, (unsigned char *)KEY, (unsigned char *)IV))
    {
        EVP_CIPHER_CTX_free(ctx);
        ereport(ERROR, (errmsg("Failed to initialize encryption")));
    }

    int block_size = EVP_CIPHER_block_size(EVP_aes_128_cbc());
    int ciphertext_len = plaintext_len + block_size;
    unsigned char *ciphertext = palloc(ciphertext_len);
    int len = 0, total_len = 0;

    if (1 != EVP_EncryptUpdate(ctx, ciphertext, &len, (unsigned char *)plaintext_str, plaintext_len))
    {
        EVP_CIPHER_CTX_free(ctx);
        ereport(ERROR, (errmsg("Encryption update failed")));
    }
    total_len = len;

    if (1 != EVP_EncryptFinal_ex(ctx, ciphertext + len, &len))
    {
        EVP_CIPHER_CTX_free(ctx);
        ereport(ERROR, (errmsg("Encryption finalization failed")));
    }
    total_len += len;
    EVP_CIPHER_CTX_free(ctx);

    bytea *result = (bytea *) palloc(total_len + VARHDRSZ);
    SET_VARSIZE(result, total_len + VARHDRSZ);
    memcpy(VARDATA(result), ciphertext, total_len);
    pfree(ciphertext);
```

Configured Visual studio properties



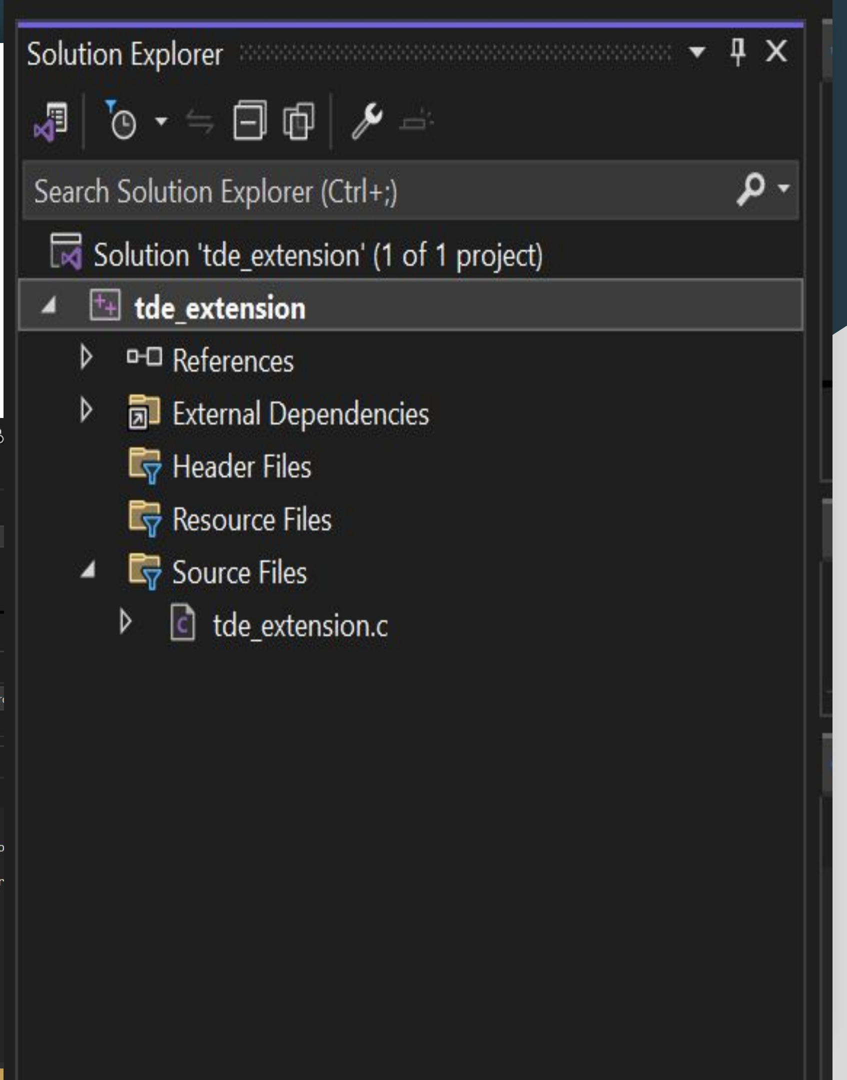
tde_extension Property Pages

Configuration: Release   Platform: Active(x64)   Configuration Manager...

- Configuration Properties
  - General
  - Advanced
  - Debugging
  - VC++ Directories
  - C/C++
    - General
    - Optimization
    - Preprocessor
    - Code Generation
    - Language
    - Precompiled Headers
    - Output Files
    - Browse Information
    - External Includes
    - Advanced
    - All Options
    - Command Line
  - Linker
  - Manifest Tool
  - XML Document Generator

Additional Include Directories	**C:\Program Files\PostgreSQL\16\include\server;C:\Program Files\PostgreS**
Additional #using Directories	
Additional BMI Directories	
Additional Module Dependencies	
Additional Header Unit Dependencies	
Scan Sources for Module Dependencies	No
Translate Includes to Imports	No
Debug Information Format	Program Database (/Zi)
Support Just My Code Debugging	No
Common Language RunTime Support	
Consume Windows Runtime Extension	
Suppress Startup Banner	Yes (/nologo)
Warning Level	**Level3 (/W3)**
Treat Warnings As Errors	No (/WX-)
Warning Version	
Diagnostics Format	Column Info (/diagnostics:column)
SDL checks	**Yes (/sdl)**
Multi-processor Compilation	
Enable Address Sanitizer	No
Enable Fuzzer Support (Experimental)	No

Additional Include Directories
Specifies one or more directories to add to the include path. Separate with ';' if more than one.   (/I[path])



Solution Explorer

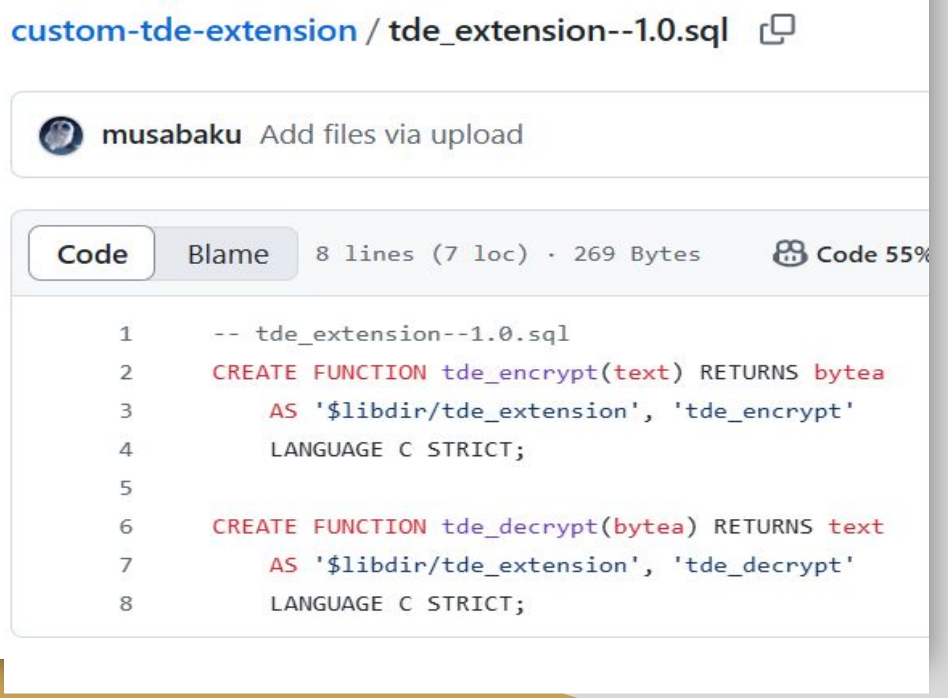
Search Solution Explorer (Ctrl+;)

- Solution 'tde_extension' (1 of 1 project)
  - **tde_extension**
    - References
    - External Dependencies
    - Header Files
    - Resource Files
    - Source Files
      - tde_extension.c

Defined Encrypt and decrypt functions

Code can be found here:

https://github.com/musabaku/custom-tde-extension/blob/main/tde_extension--1.0.sql

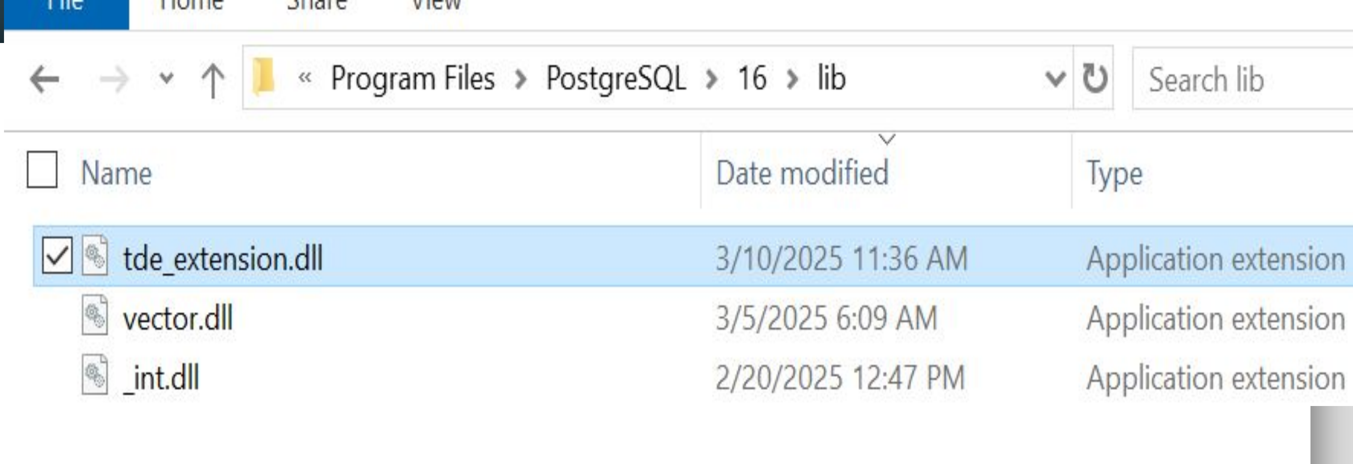


custom-tde-extension / tde_extension--1.0.sql

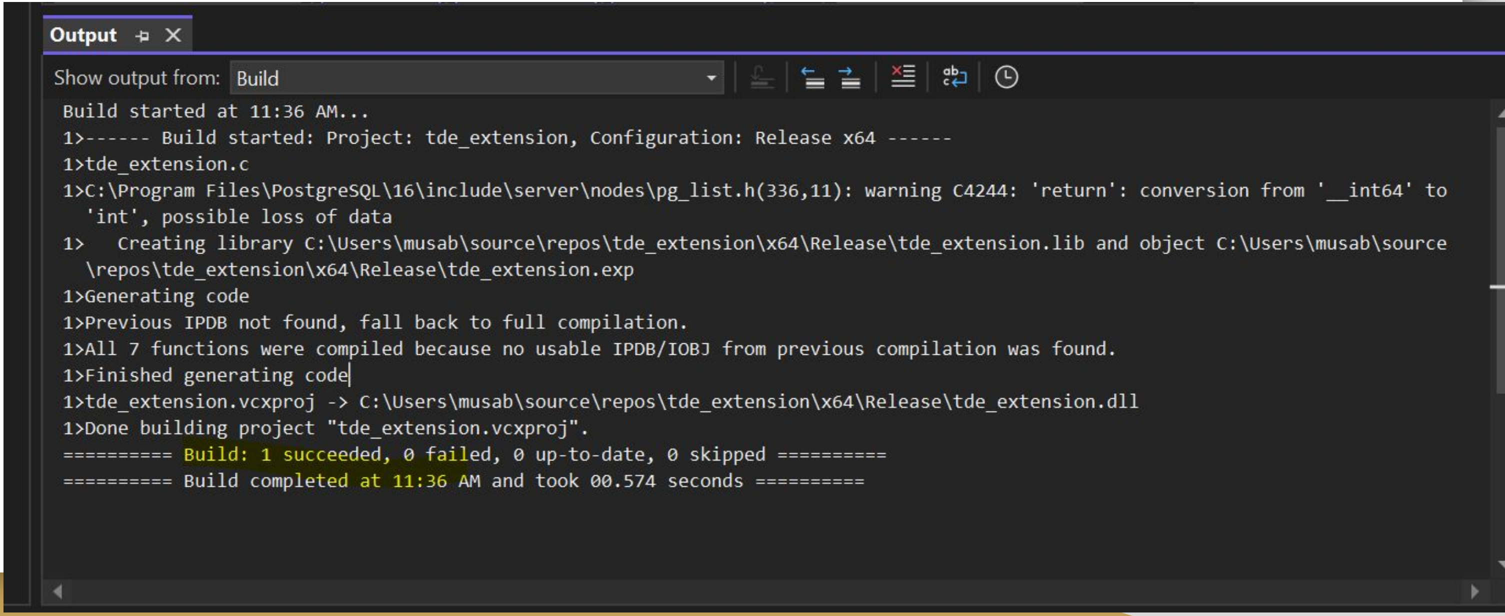
musabaku Add files via upload

```sql
-- tde_extension--1.0.sql
CREATE FUNCTION tde_encrypt(text) RETURNS bytea
    AS '$libdir/tde_extension', 'tde_encrypt'
    LANGUAGE C STRICT;

CREATE FUNCTION tde_decrypt(bytea) RETURNS text
    AS '$libdir/tde_extension', 'tde_decrypt'
    LANGUAGE C STRICT;
```

Compiled & Placed files in relevant folders

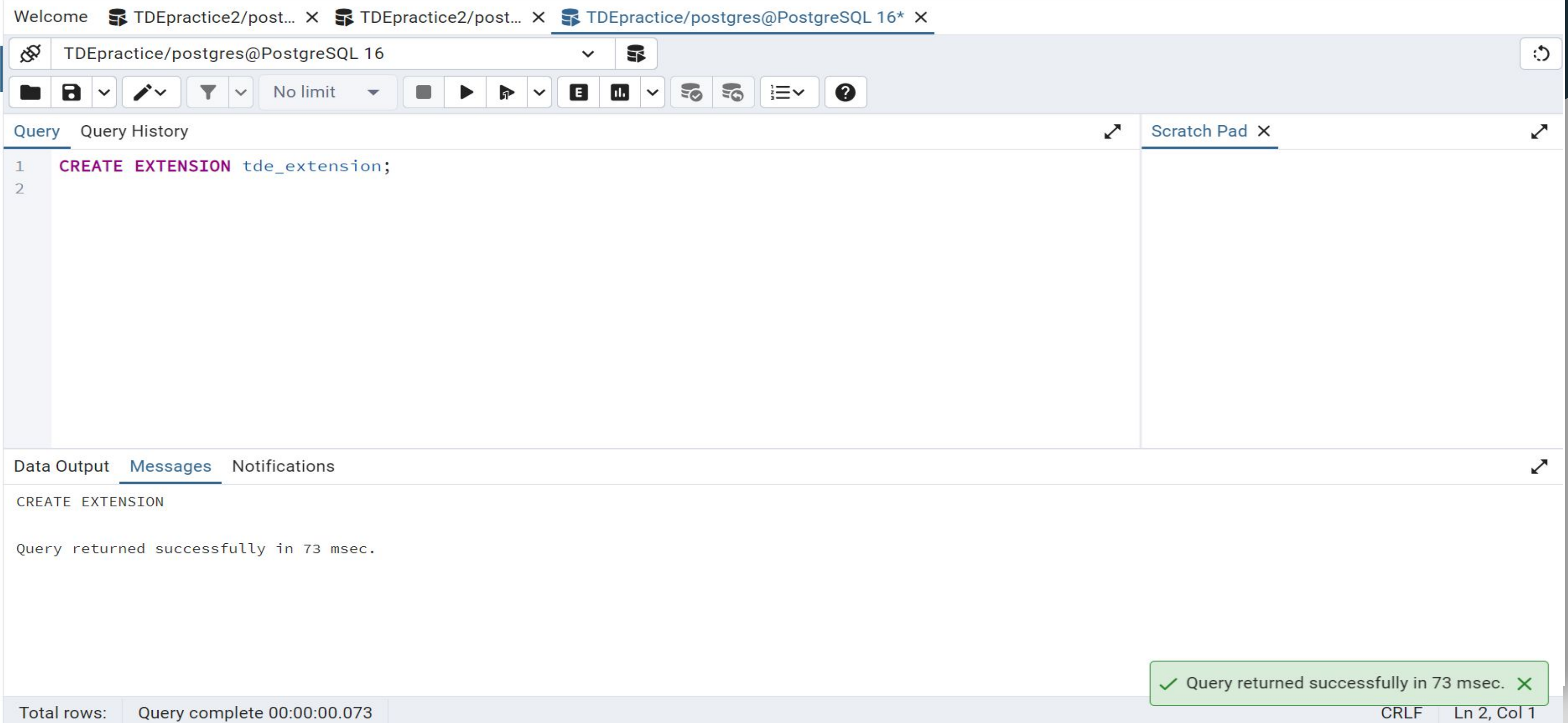


	Name	Date modified	Type
☑	tde_extension.dll	3/10/2025 11:36 AM	Application extension
	vector.dll	3/5/2025 6:09 AM	Application extension
	_int.dll	2/20/2025 12:47 PM	Application extension



```
Build started at 11:36 AM...
1>------ Build started: Project: tde_extension, Configuration: Release x64 ------
1>tde_extension.c
1>C:\Program Files\PostgreSQL\16\include\server\nodes\pg_list.h(336,11): warning C4244: 'return': conversion from '__int64' to
  'int', possible loss of data
1>   Creating library C:\Users\musab\source\repos\tde_extension\x64\Release\tde_extension.lib and object C:\Users\musab\source
  \repos\tde_extension\x64\Release\tde_extension.exp
1>Generating code
1>Previous IPDB not found, fall back to full compilation.
1>All 7 functions were compiled because no usable IPDB/IOBJ from previous compilation was found.
1>Finished generating code
1>tde_extension.vcxproj -> C:\Users\musab\source\repos\tde_extension\x64\Release\tde_extension.dll
1>Done building project "tde_extension.vcxproj".
========== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped ==========
========== Build completed at 11:36 AM and took 00.574 seconds ==========
```

Creating custom extension in pgadmin



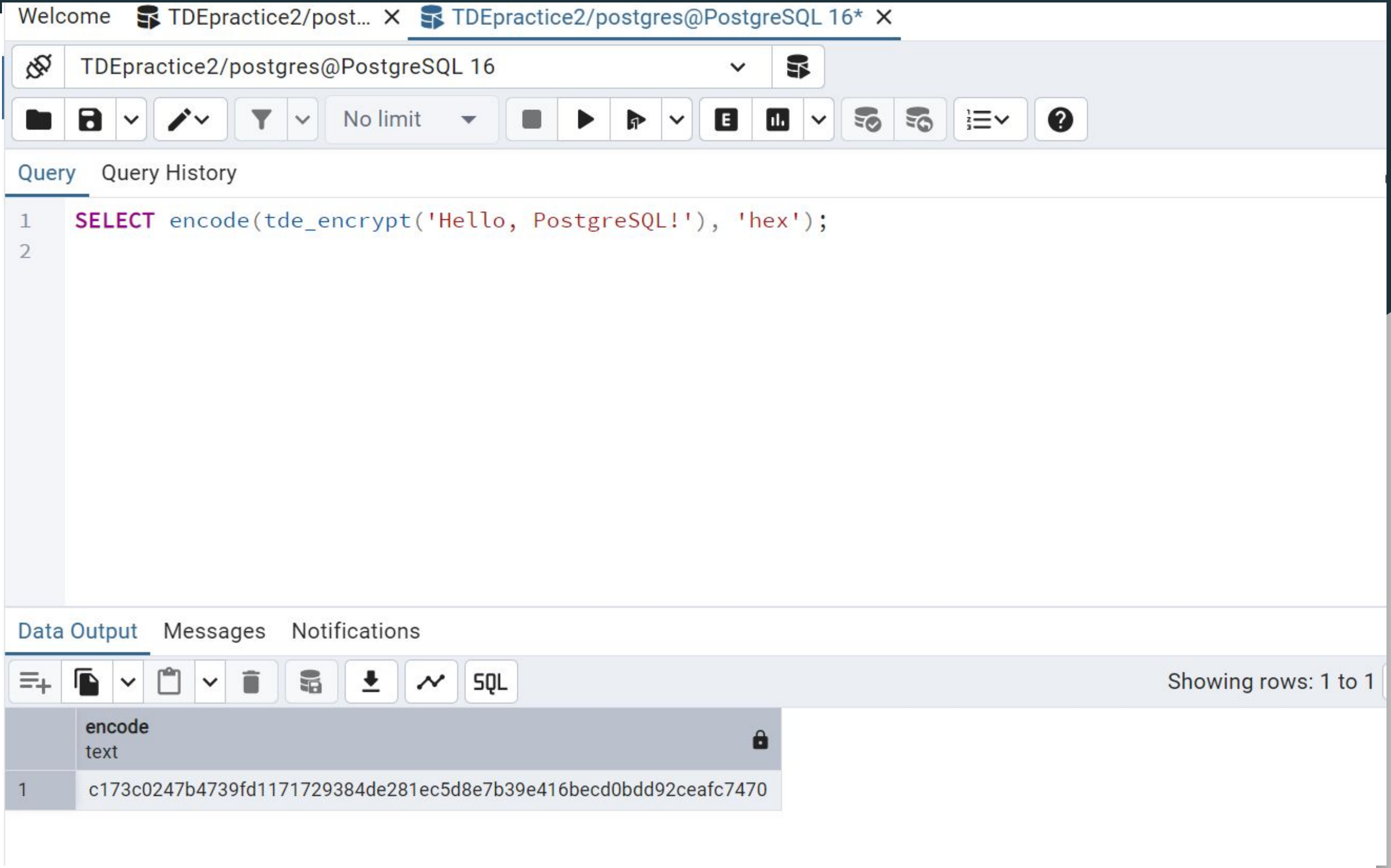
```
CREATE EXTENSION tde_extension;
```

```
CREATE EXTENSION

Query returned successfully in 73 msec.
```

✓ Query returned successfully in 73 msec.

Total rows: Query complete 00:00:00.073 CRLF Ln 2, Col 1

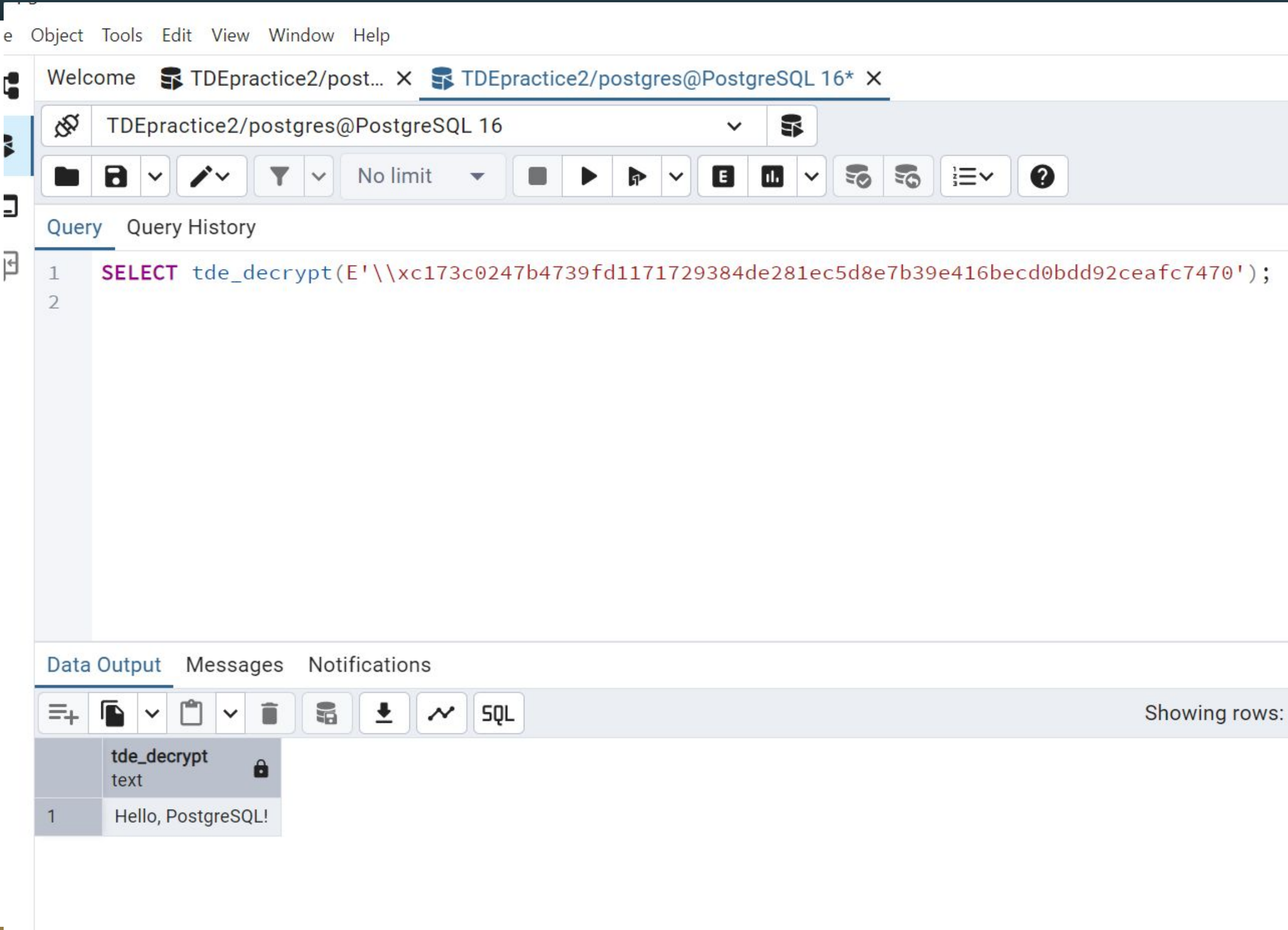
Testing Encrypt Function in PgAdmin



```
SELECT encode(tde_encrypt('Hello, PostgreSQL!'), 'hex');
```

	encode text
1	c173c0247b4739fd1171729384de281ec5d8e7b39e416becd0bdd92ceafc7470

Testing Decrypt Function in PgAdmin


e Object Tools Edit View Window Help
Welcome
TDEpractice2/post...
TDEpractice2/postgres@PostgreSQL 16*
TDEpractice2/postgres@PostgreSQL 16
No limit
Query
Query History
Data Output
Messages
Notifications
SQL
Showing rows:

```
SELECT tde_decrypt(E'\\xc173c0247b4739fd1171729384de281ec5d8e7b39e416becd0bdd92ceafc7470');
```

	tde_decrypt text
1	Hello, PostgreSQL!