

BẢO MẬT CƠ SỞ DỮ LIỆU

Lab05 –Transparent Data Encryption - TDE

Sinh viên:

Đỗ Trọng Nghĩa - 18120477



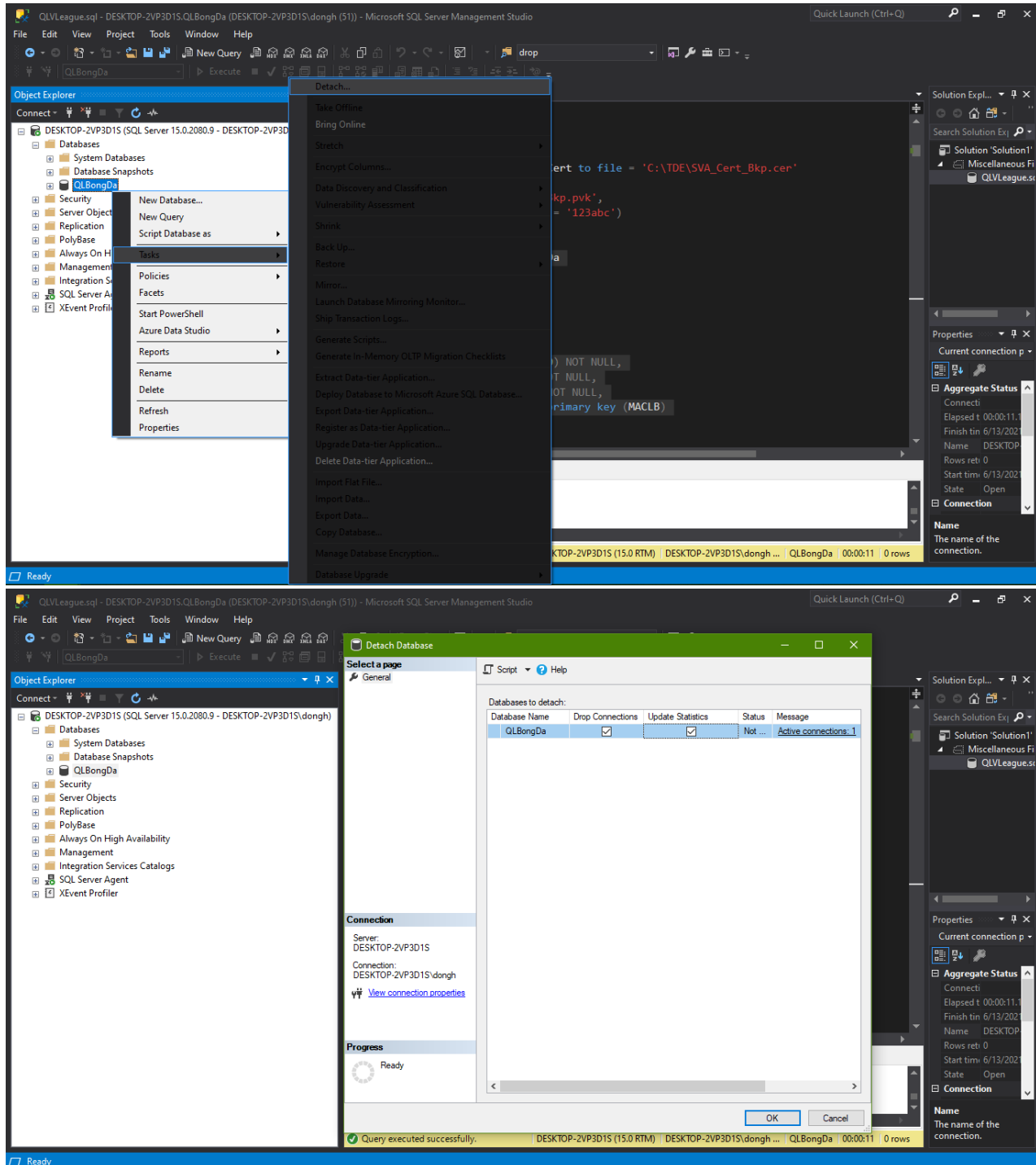
Khoa Công nghệ Thông tin
Đại học Khoa học Tự nhiên TP HCM

I. Attach – Detach & Backup – Restore với Database không có TDE	3
I.1. Attach – Detach	3
I.2. Backup – Restore.....	8
II. Mã hóa TDE cho Database.....	15
III. Attach – Detach & Backup – Restore với Database có TDE	16
III.1. Attach – Detach	16
III.2. Backup – Restore	18
III.3. Giải pháp.....	22

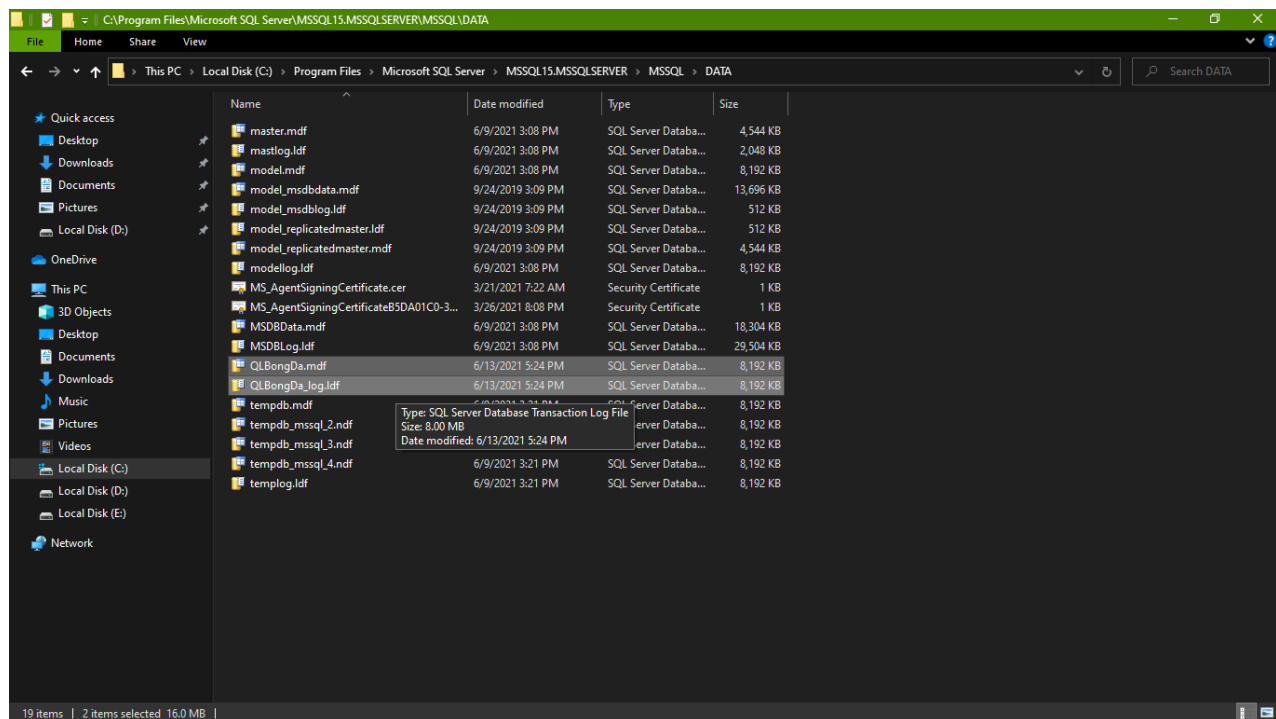
I. Attach – Detach & Backup – Restore với Database không có TDE

I.1. Attach – Detach

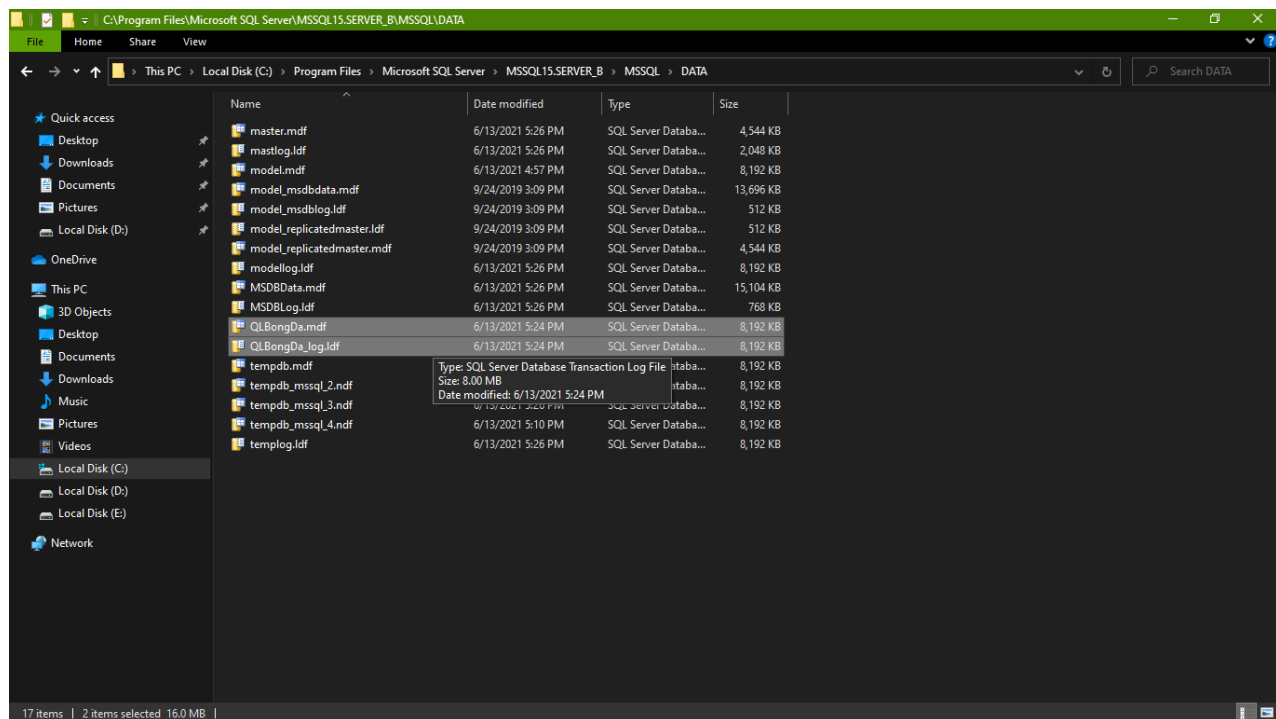
- Thực hiện Detach ở Server Chính



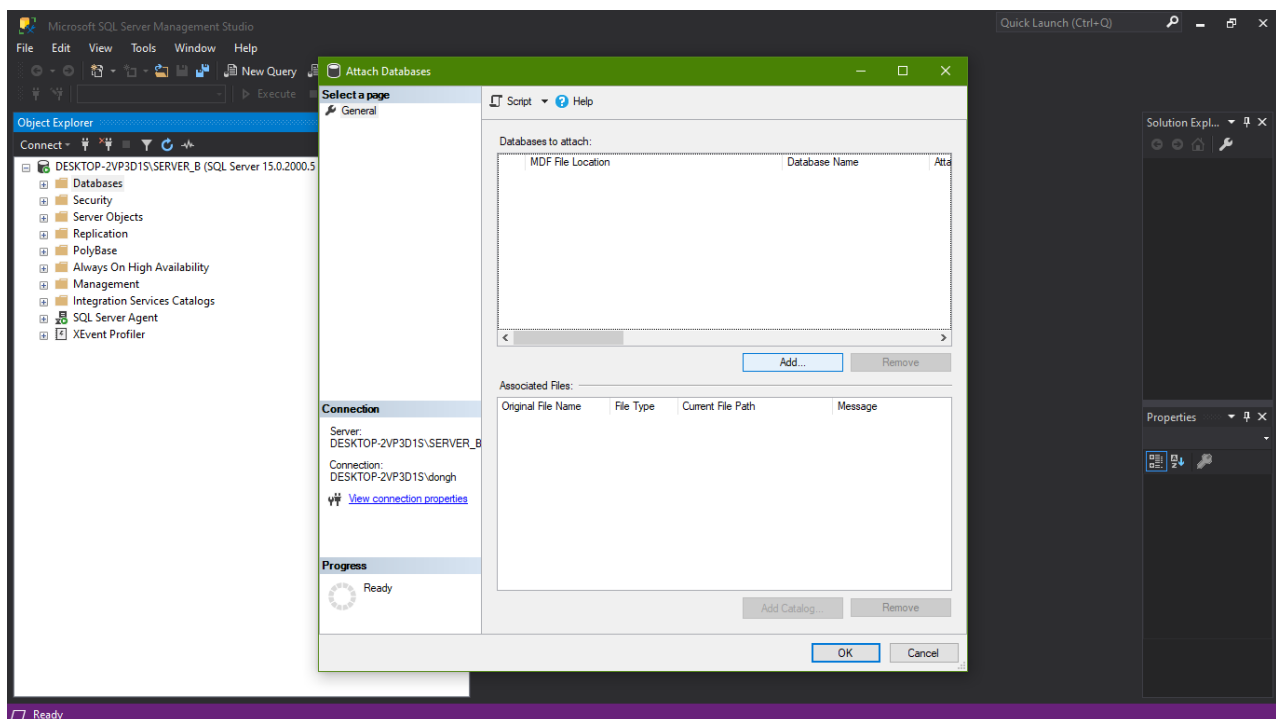
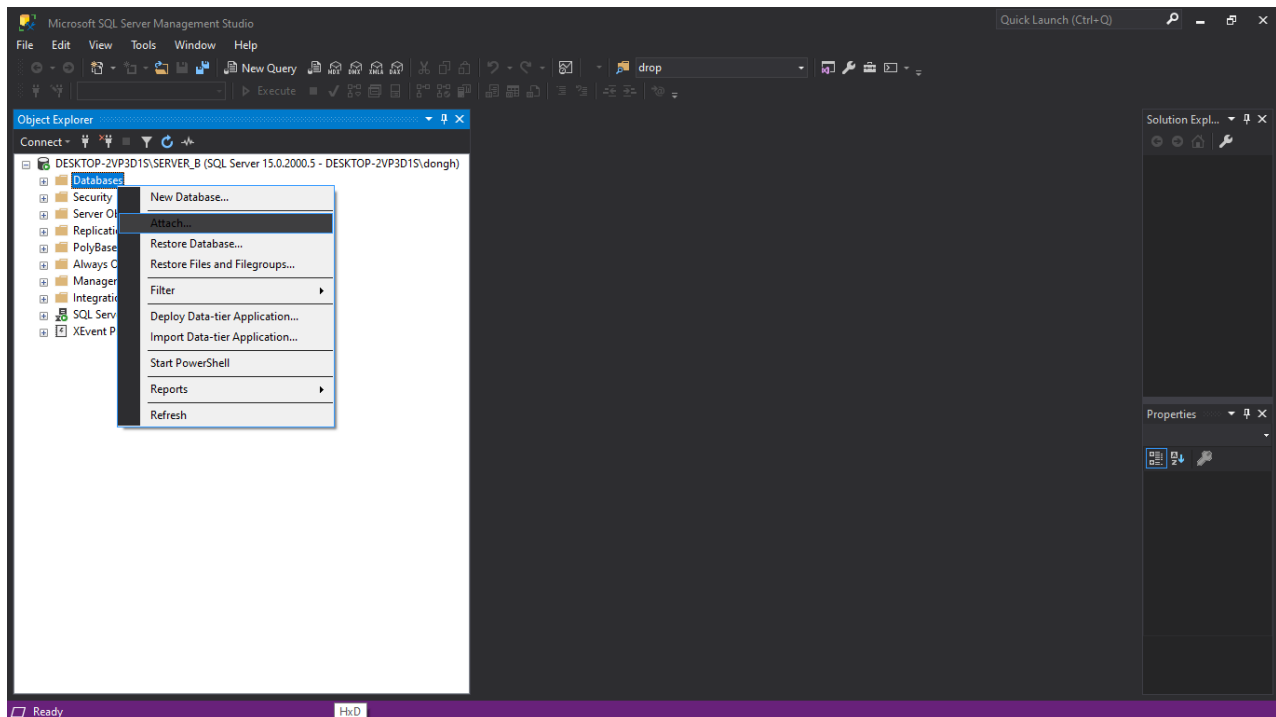
- Copy các file .mdf và .ldf từ folder của Server chính qua folder của Server_B



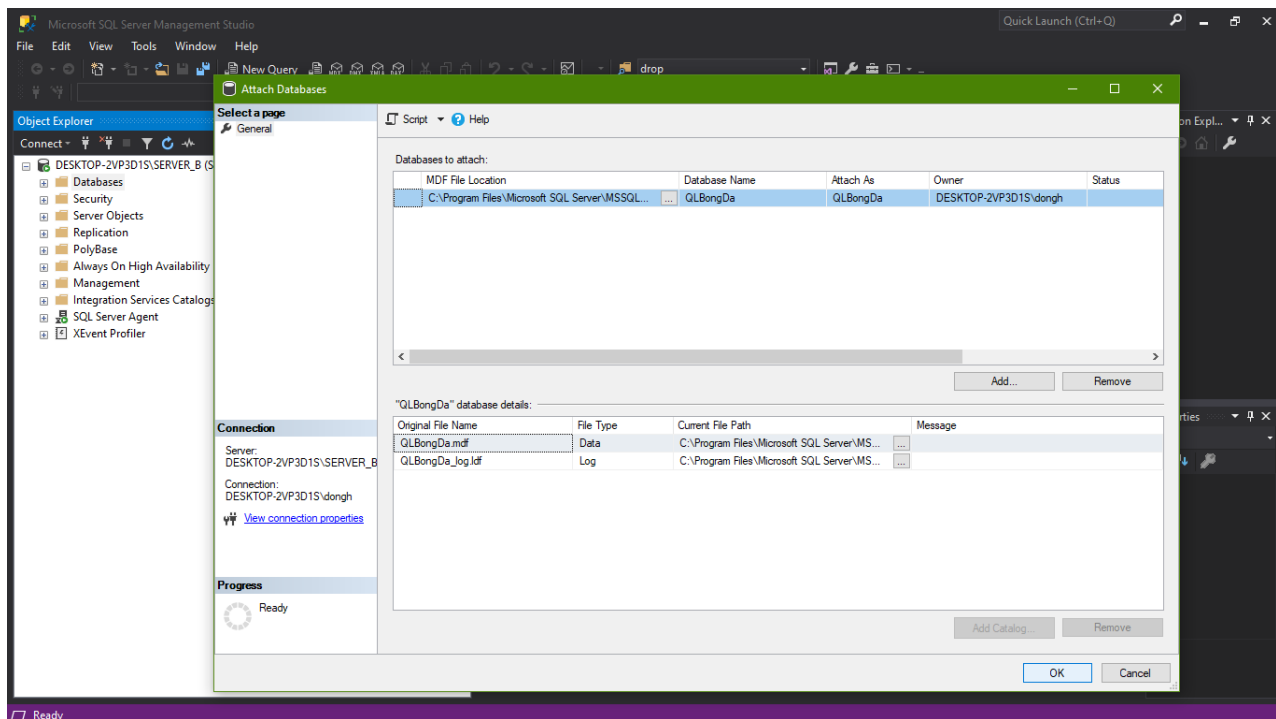
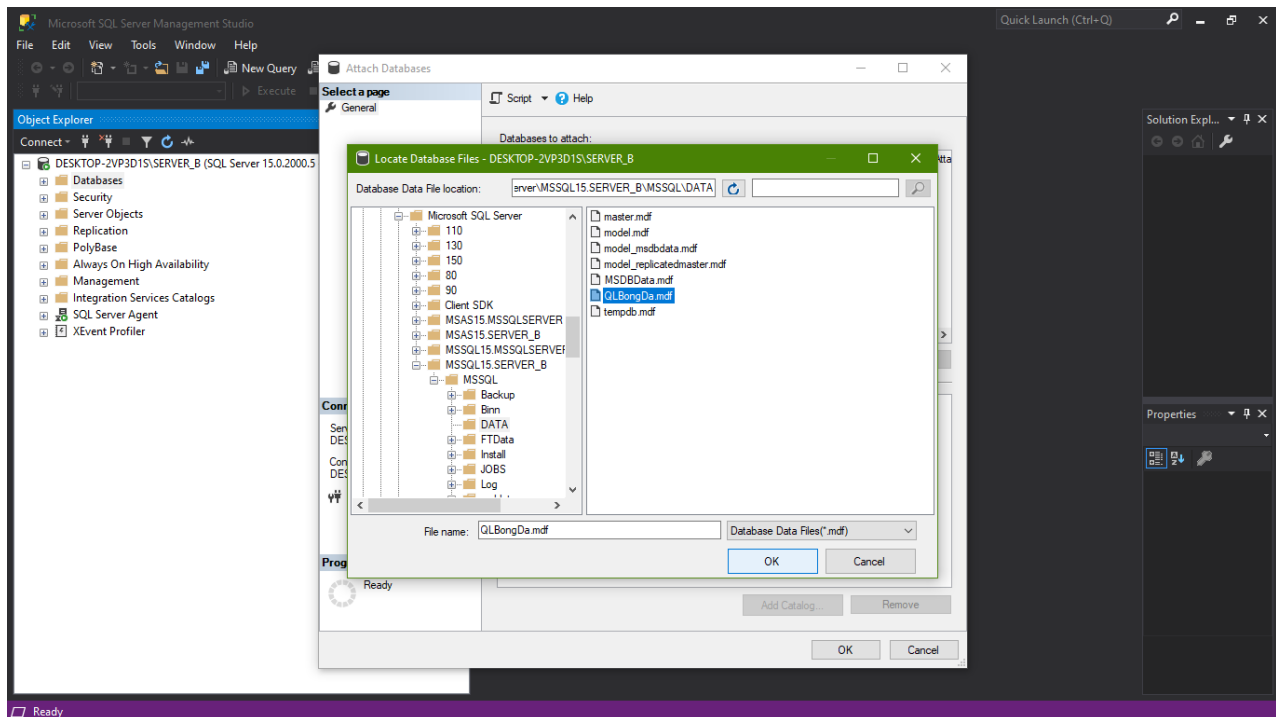
- Folder Server_B



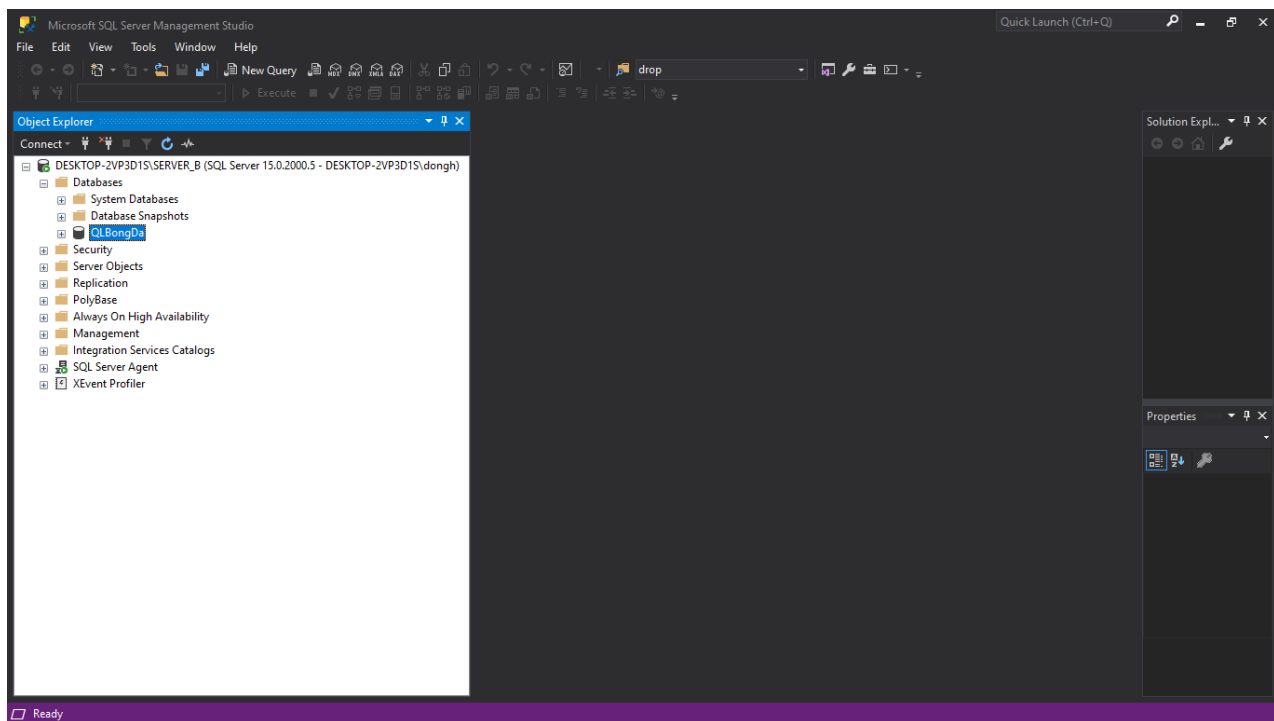
- Thực hiện Attach tại Server_B



- Chọn file để Attach

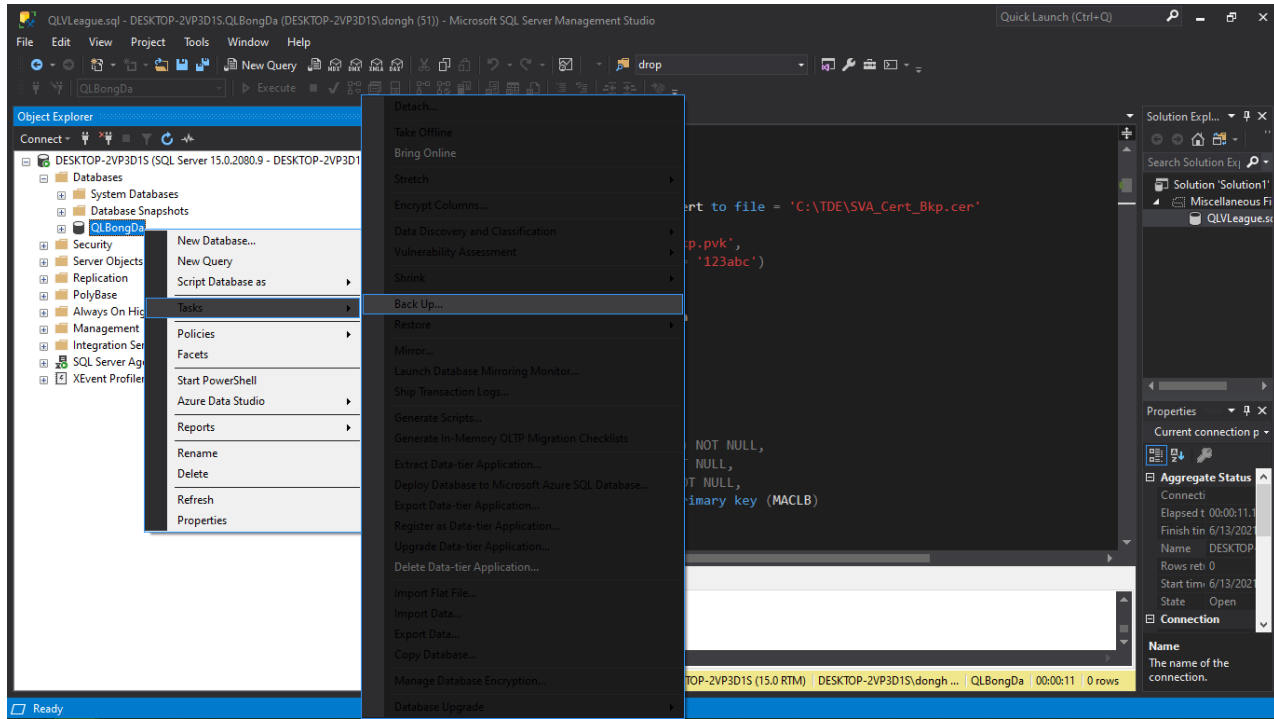


- Attach thành công

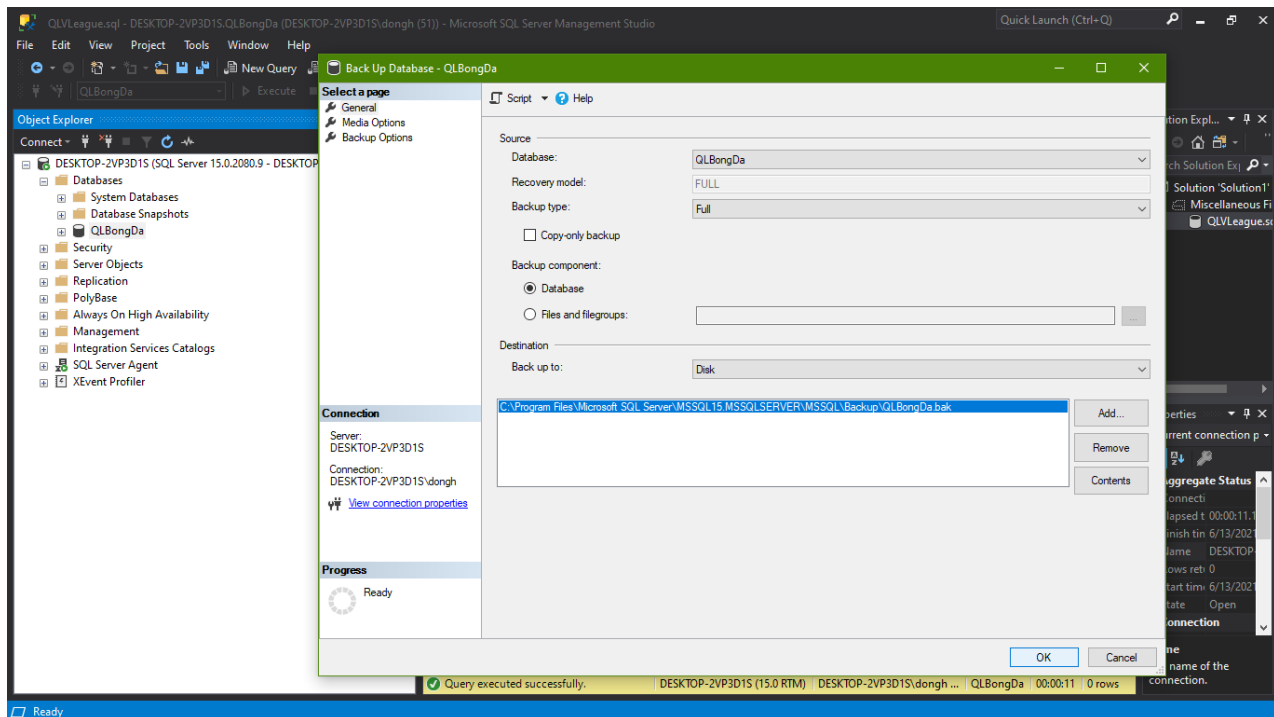


I.2. Backup – Restore

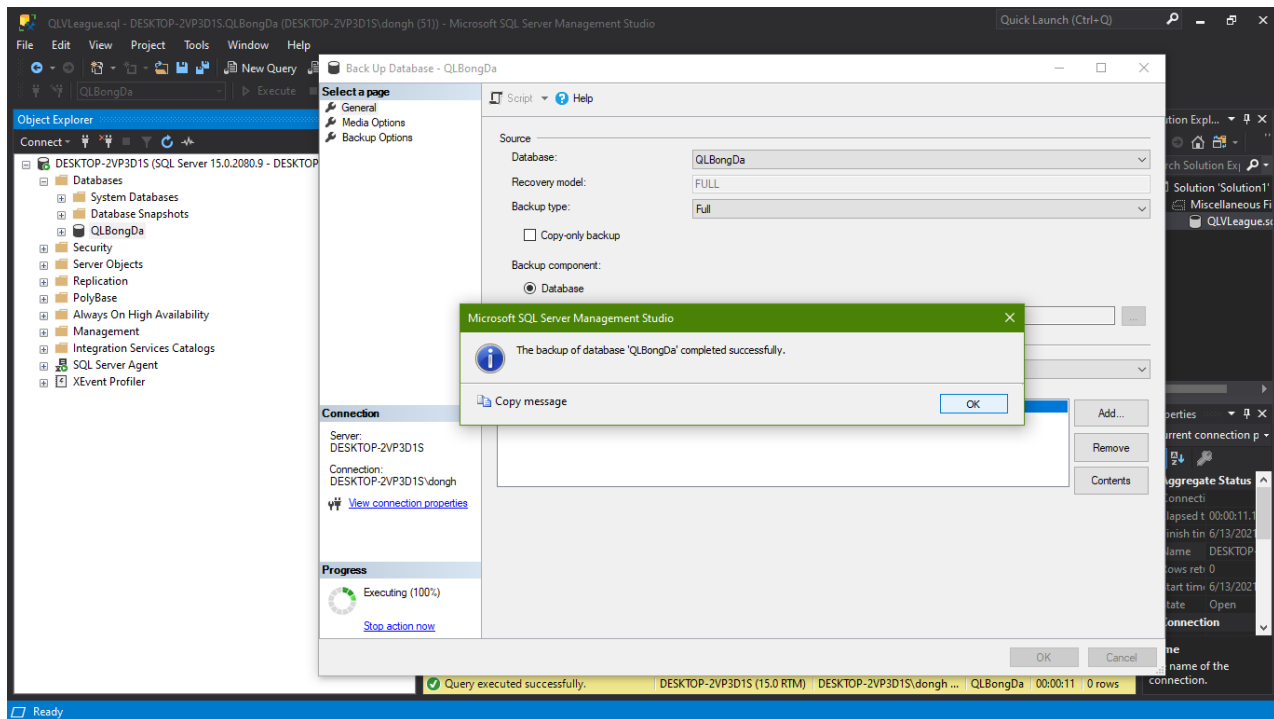
- Tại Server chính chọn Back Up Database (QLBongDa)



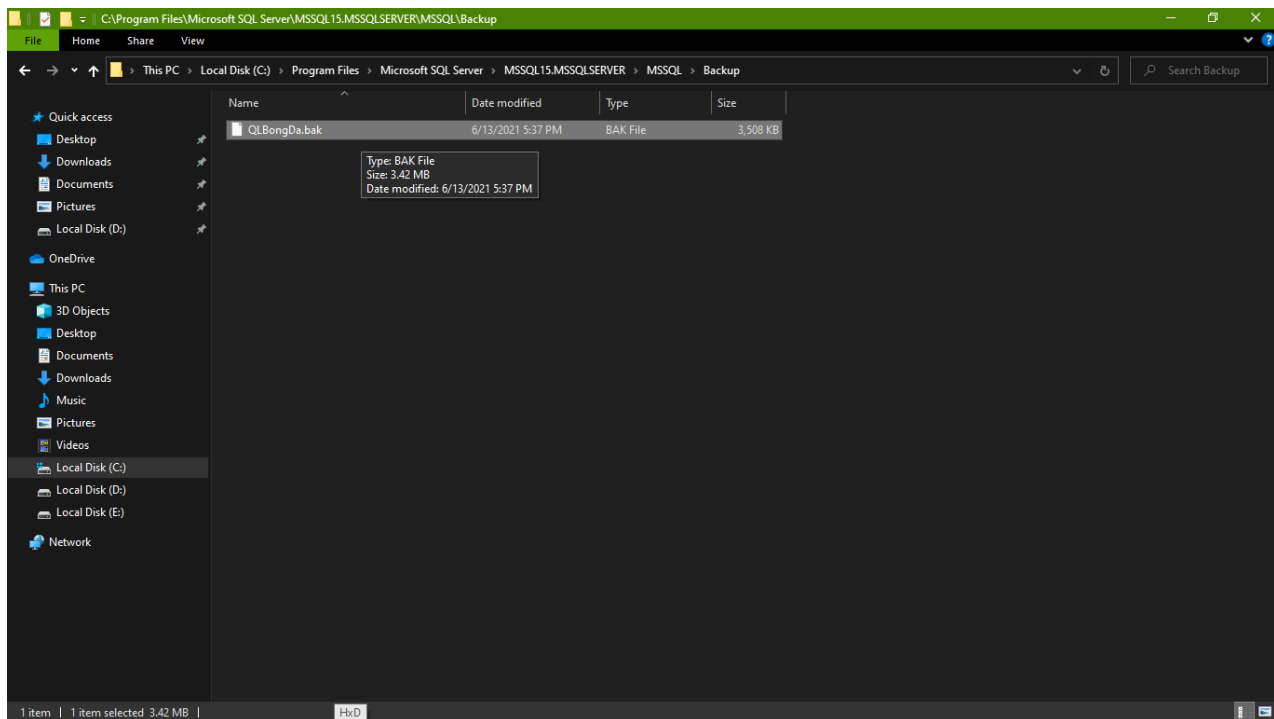
- Backup type là Full

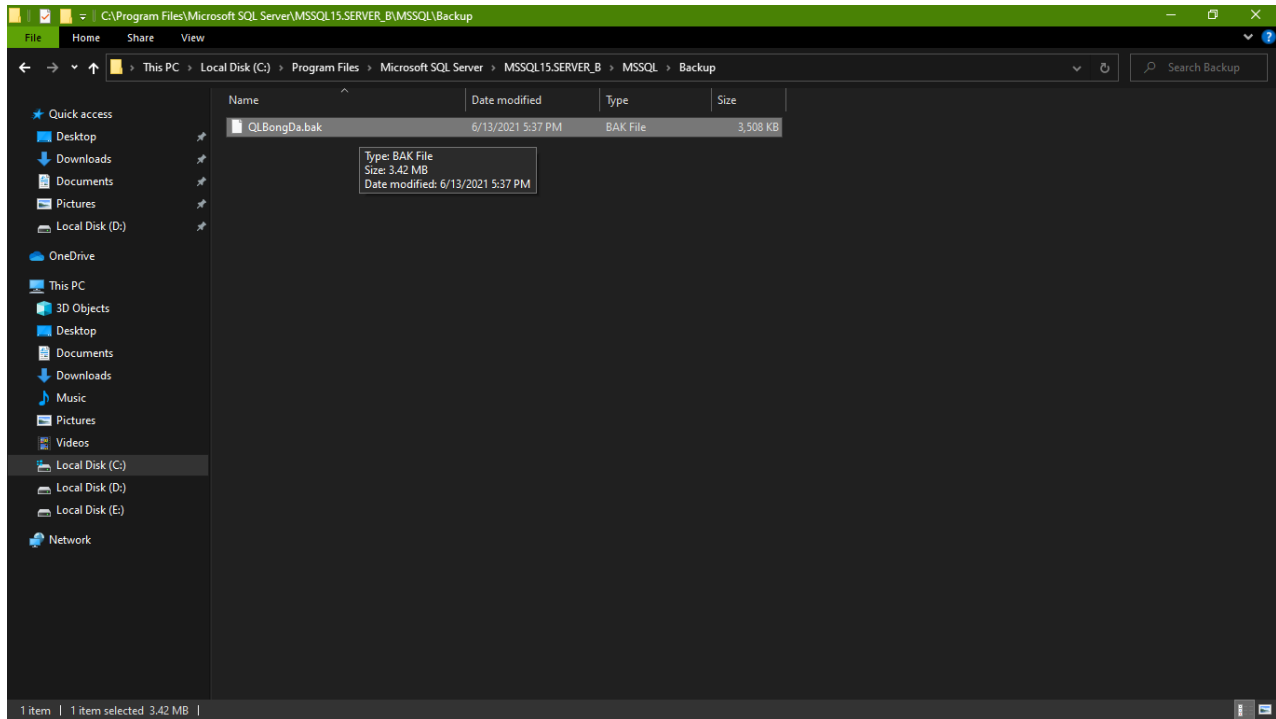


- Tạo file Backup thành công

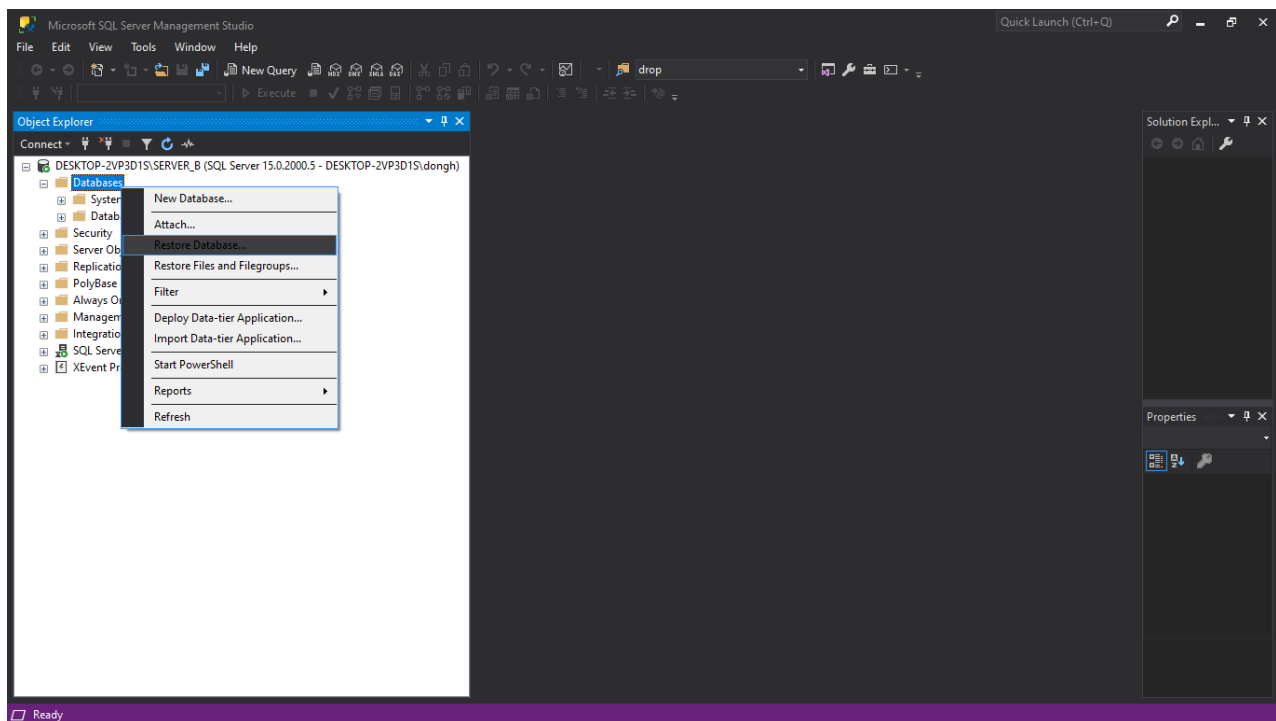


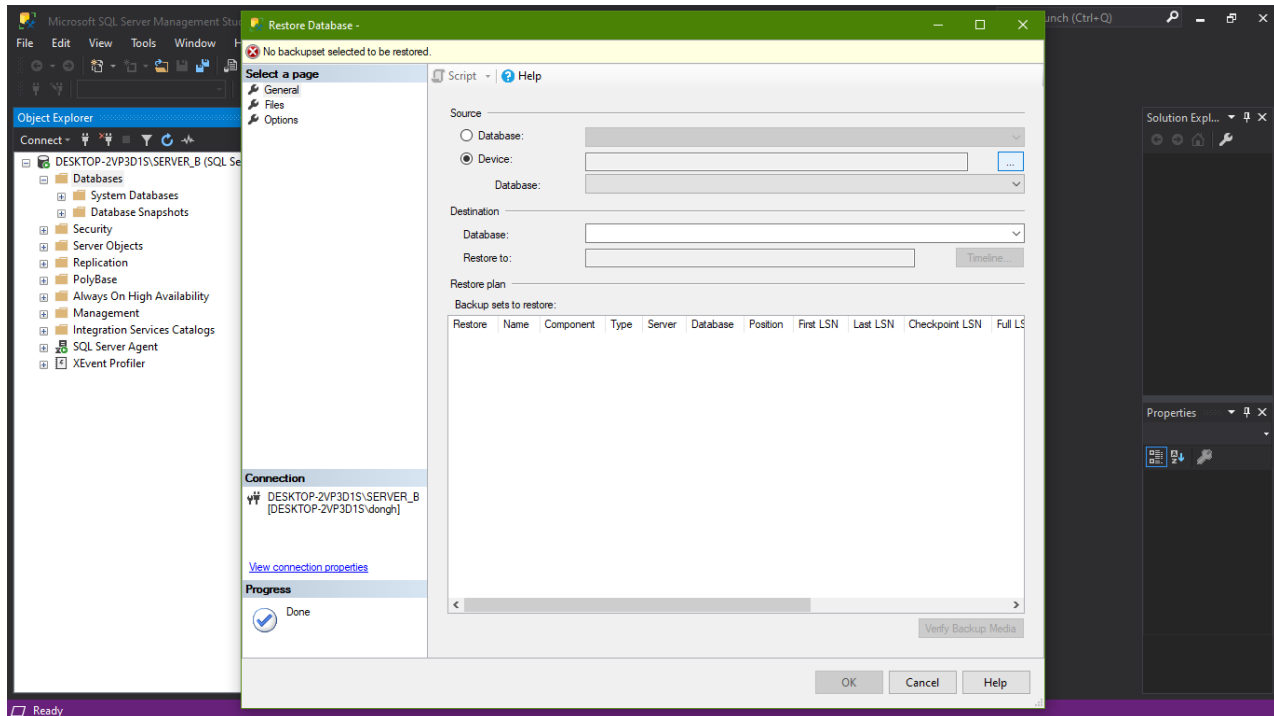
- Copy file Backup từ folder Server chính sang folder Server_B



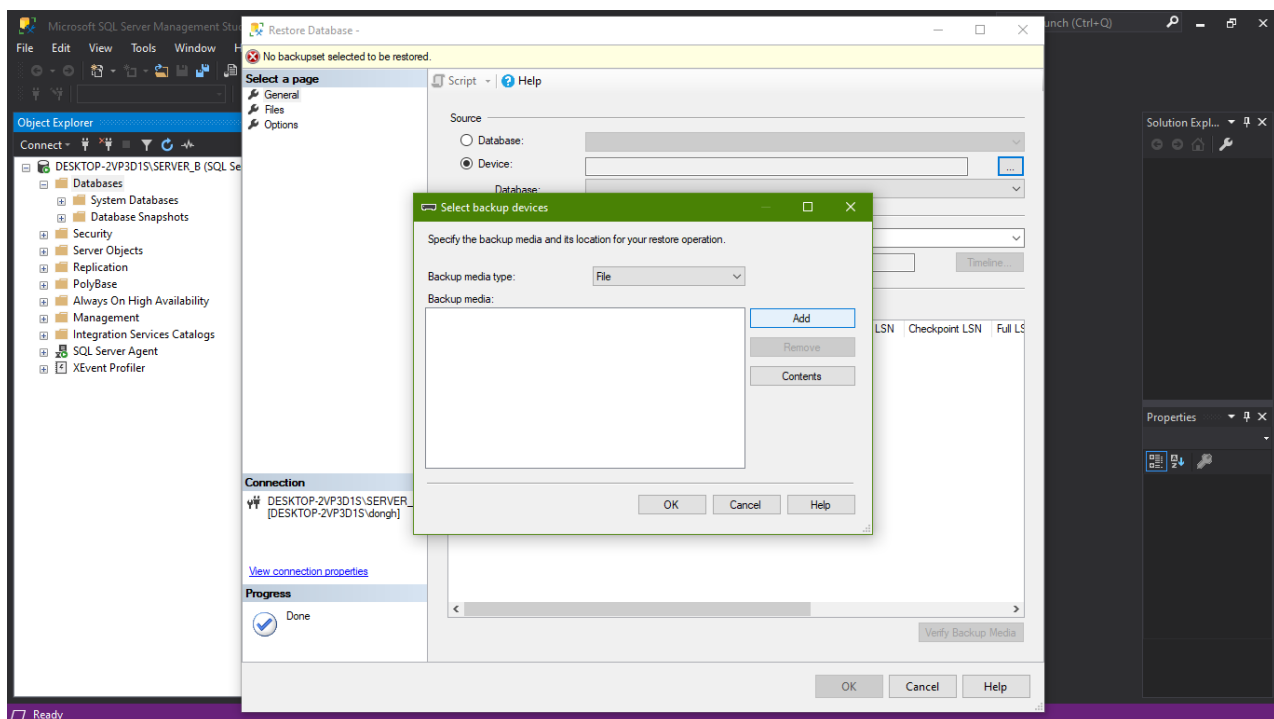


- Thực hiện Restore tại Server_B

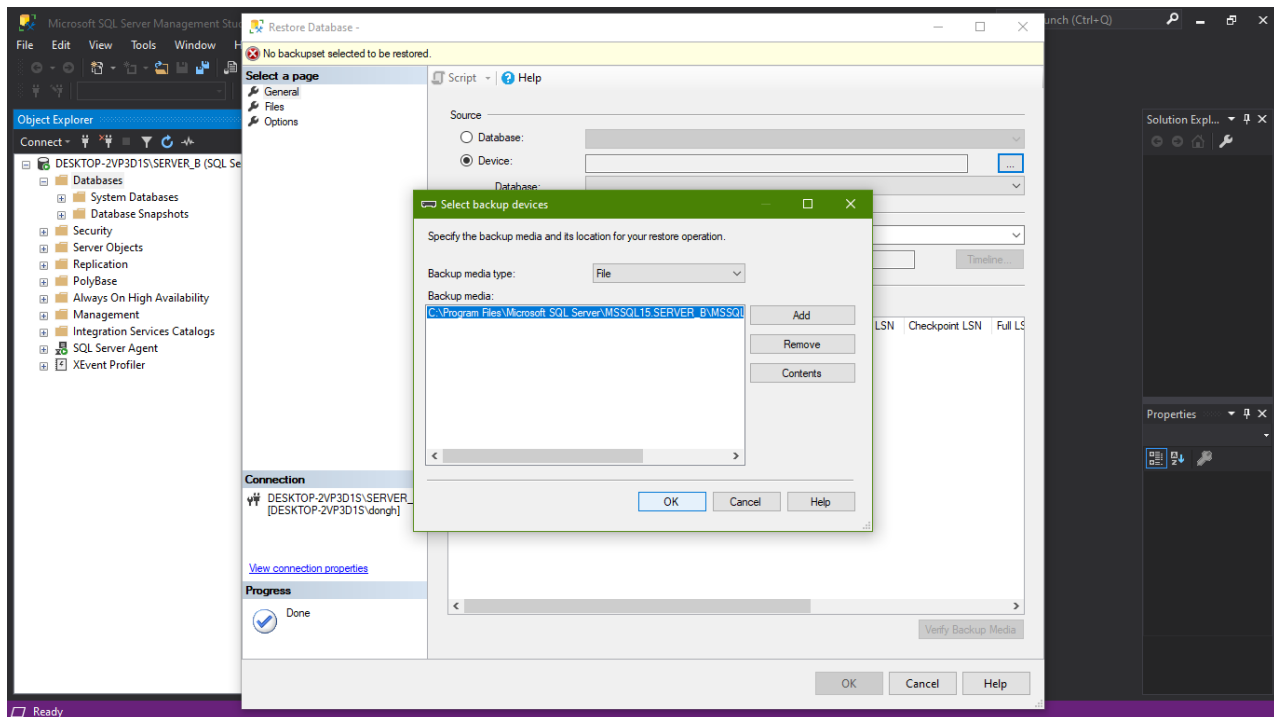
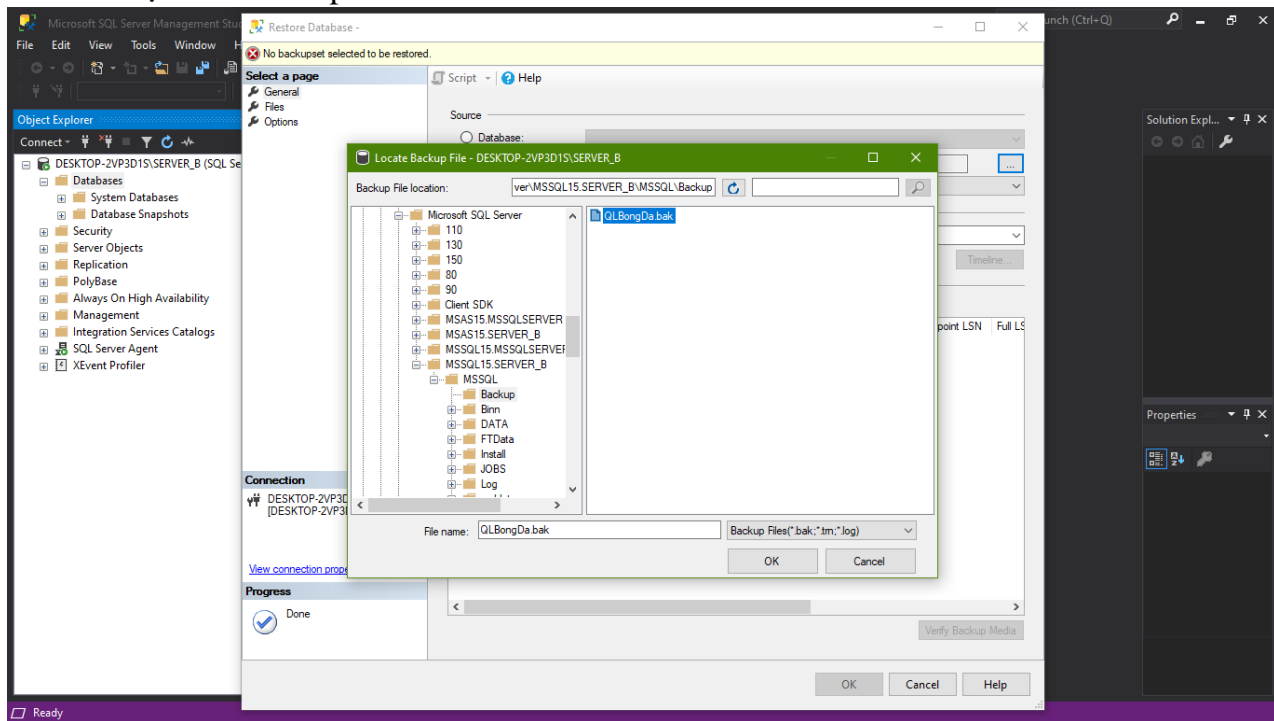




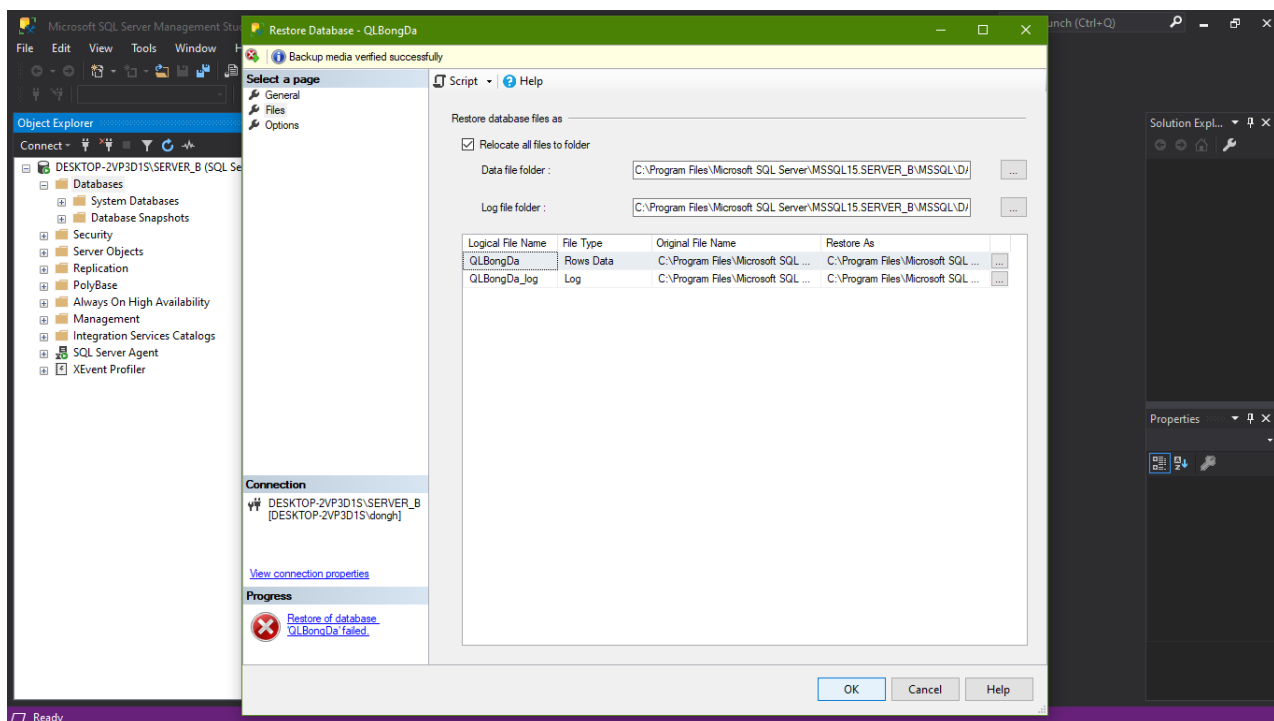
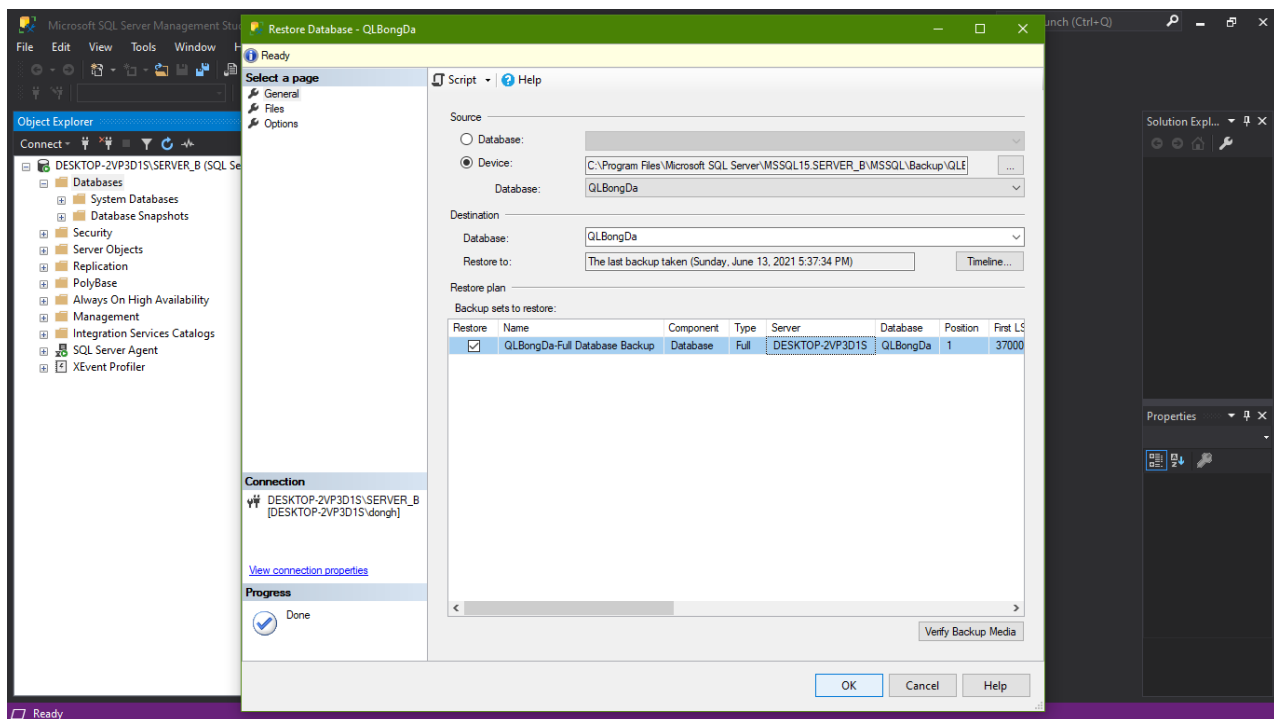
- Thêm file Backup

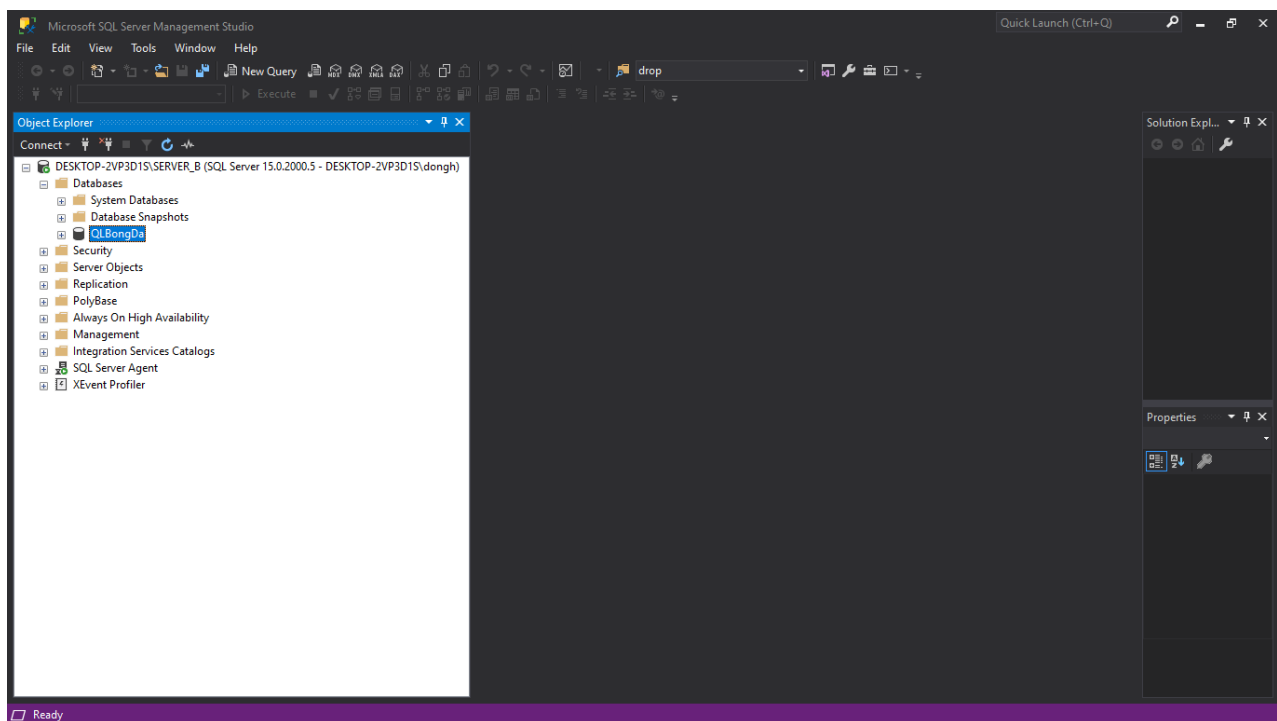
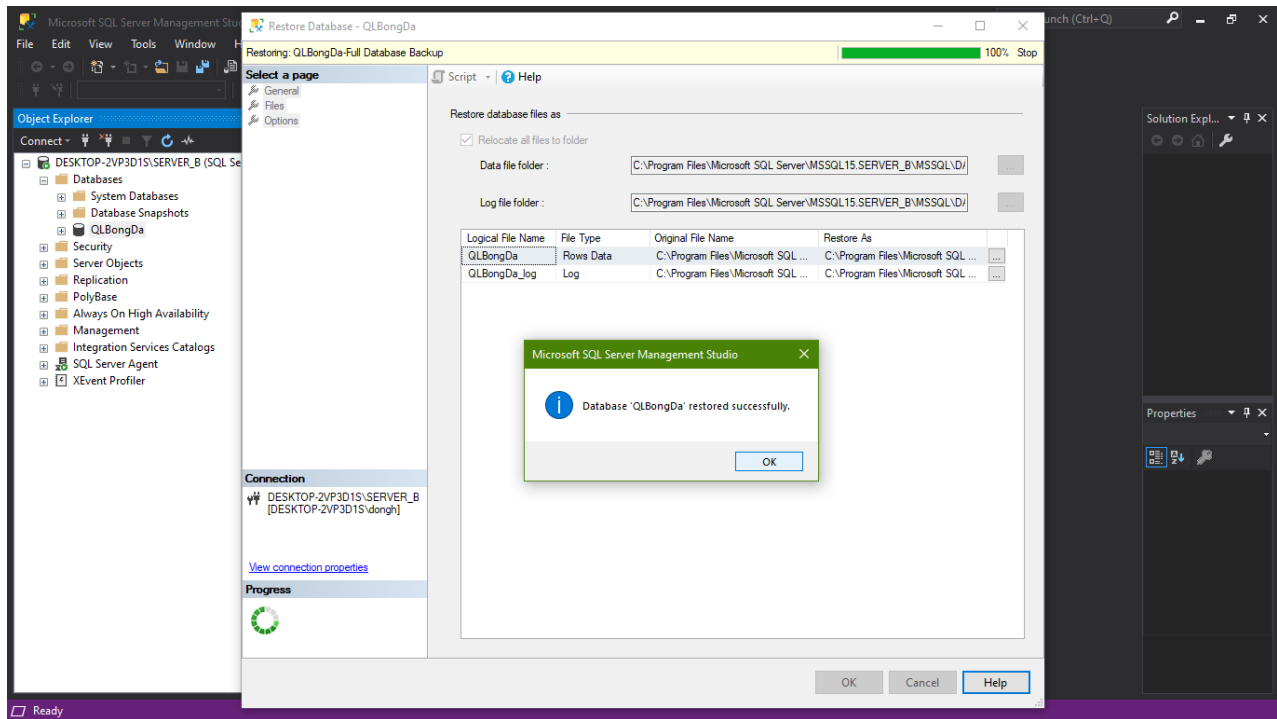


- Chọn file Backup



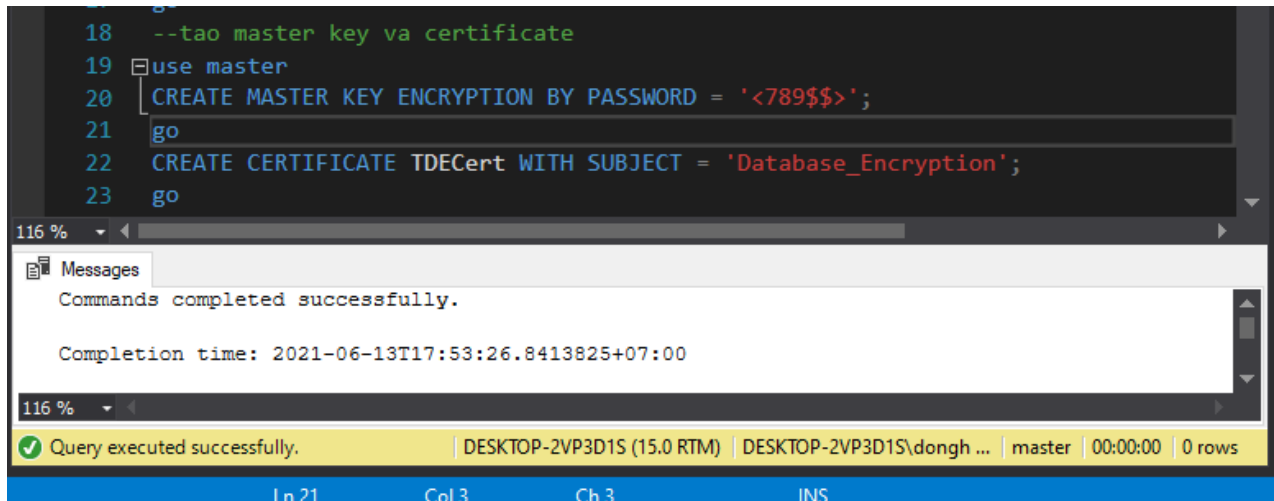
- Restore thành công (cần phải Relocate all files to folder)





II. Mã hóa TDE cho Database

- Ở Server Chính



```
18 --tao master key va certificate
19 use master
20 CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<789$$>';
21 go
22 CREATE CERTIFICATE TDECert WITH SUBJECT = 'Database_Encryption';
23 go
```

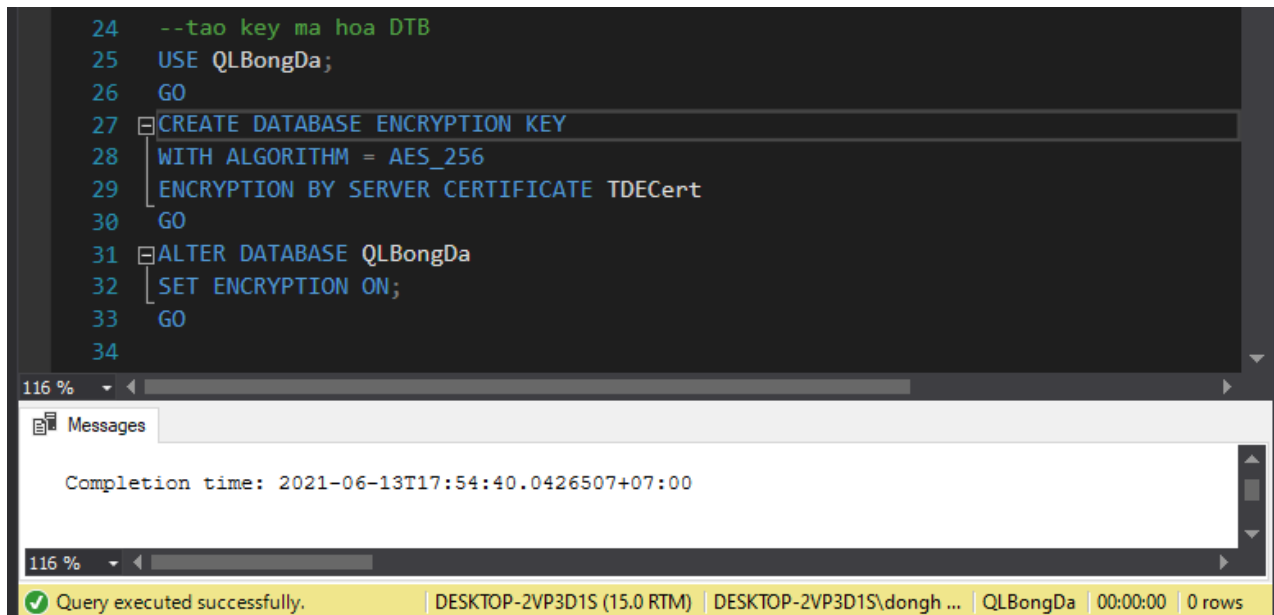
Messages

Commands completed successfully.

Completion time: 2021-06-13T17:53:26.8413825+07:00

Query executed successfully. | DESKTOP-2VP3D1S (15.0 RTM) | DESKTOP-2VP3D1S\dongh ... | master | 00:00:00 | 0 rows

Ln 21 Col 3 Ch 3 INS



```
24 --tao key ma hoa DTB
25 USE QL BongDa;
26 GO
27 CREATE DATABASE ENCRYPTION KEY
28 WITH ALGORITHM = AES_256
29 ENCRYPTION BY SERVER CERTIFICATE TDECert
30 GO
31 ALTER DATABASE QL BongDa
32 SET ENCRYPTION ON;
33 GO
34
```

Messages

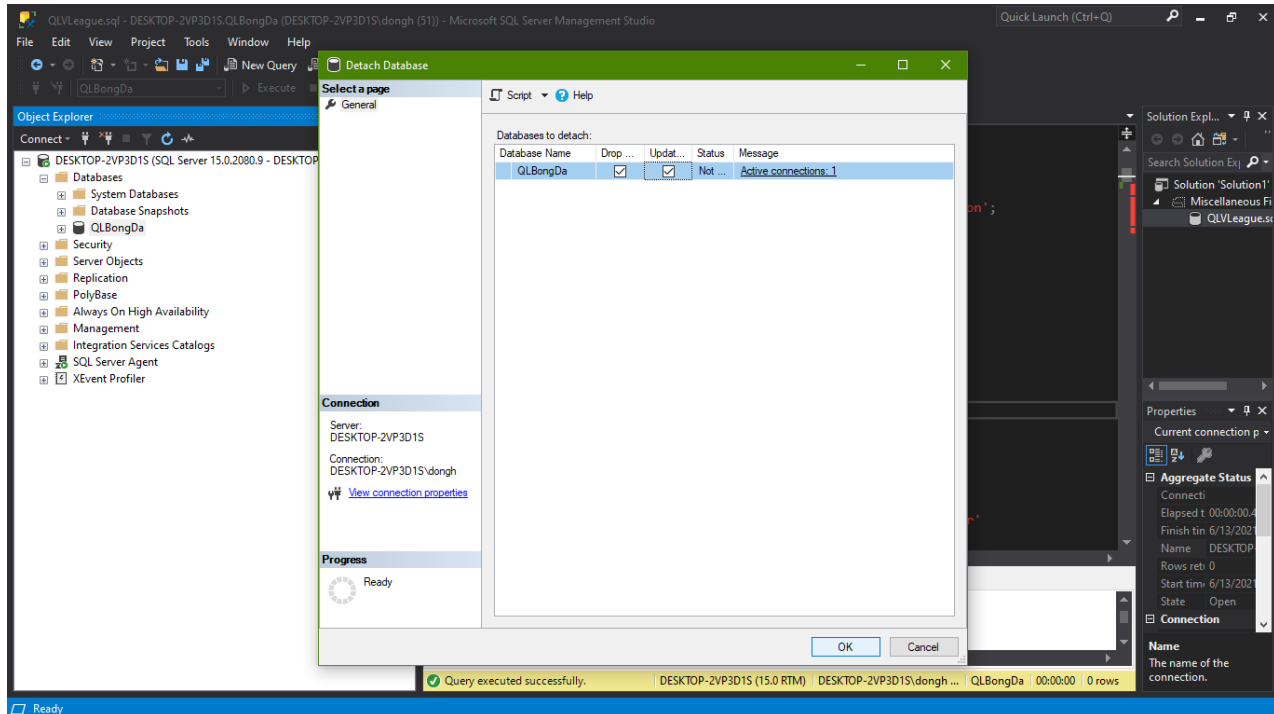
Completion time: 2021-06-13T17:54:40.0426507+07:00

Query executed successfully. | DESKTOP-2VP3D1S (15.0 RTM) | DESKTOP-2VP3D1S\dongh ... | QL BongDa | 00:00:00 | 0 rows

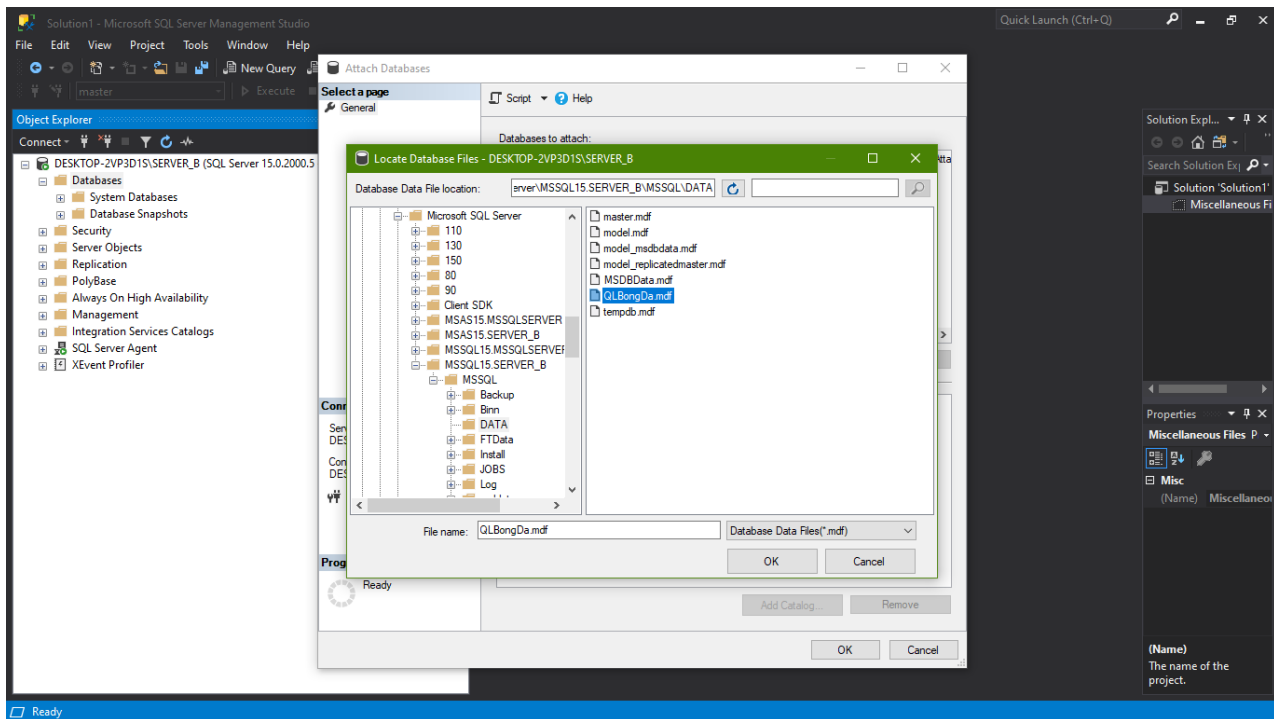
III. Attach – Detach & Backup – Restore với Database có TDE

III.1. Attach – Detach

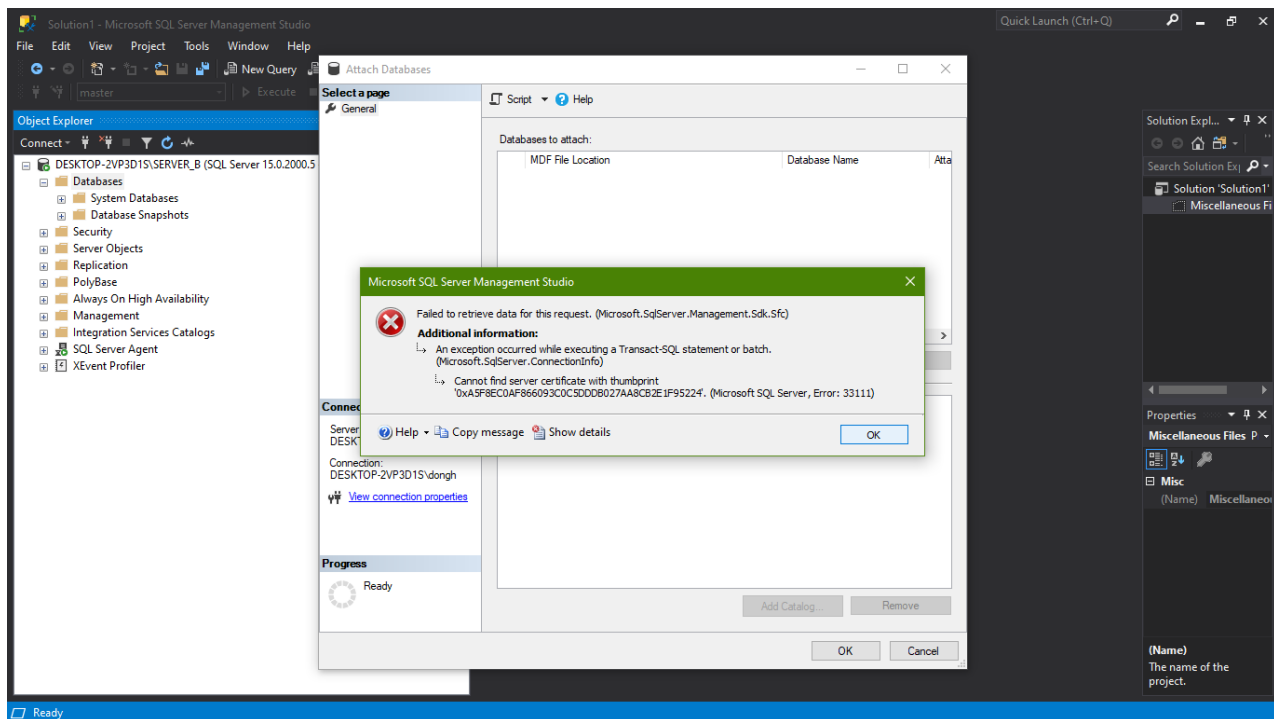
- Ở Server chính thực hiện Dettach, sau đó copy các file .mdf và .ldf vừ folder Server chính sang Server_B (tương tự như phần đầu)



- Tại Server_B tiến hành chọn file Attach

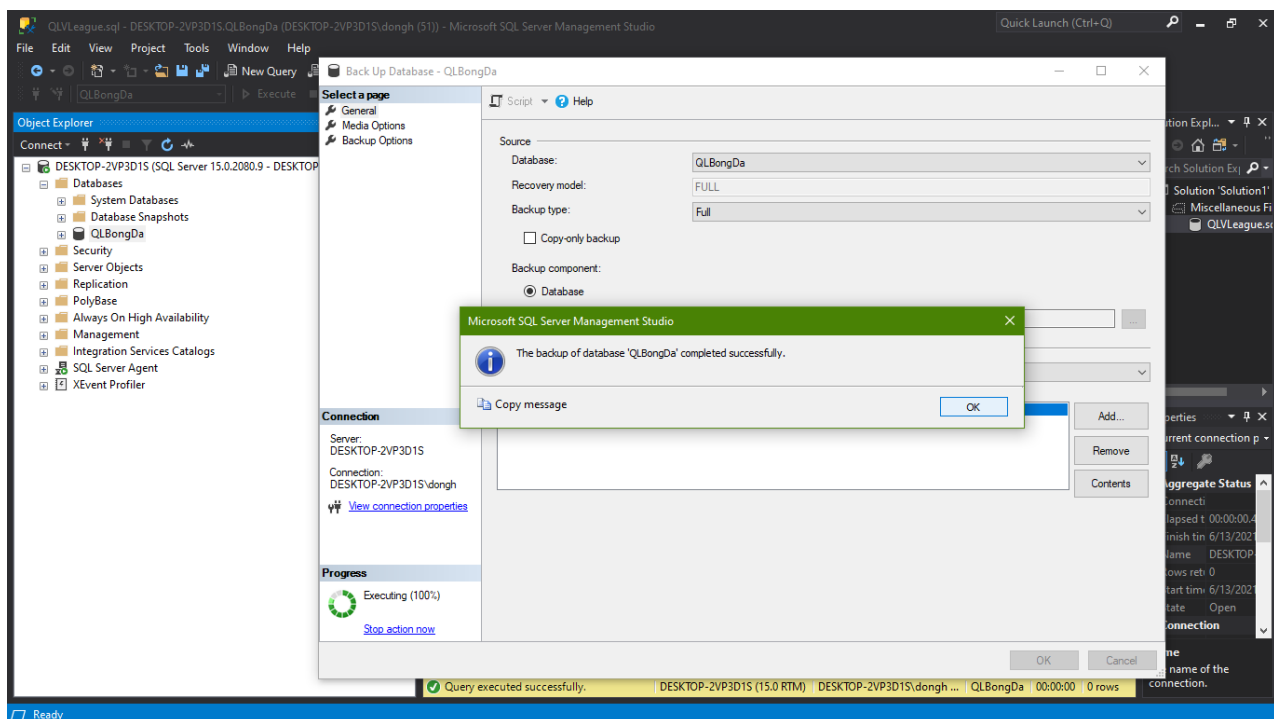
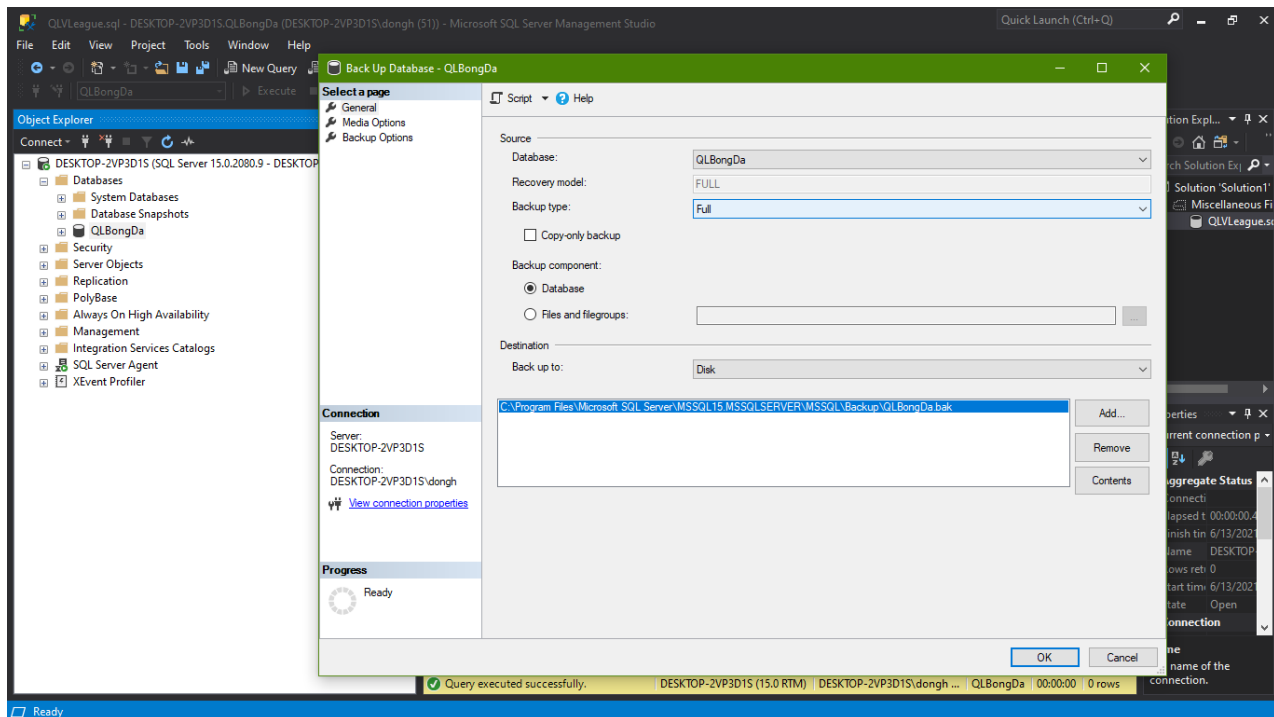


- Attach thất bại Certificate và Key mã hóa Database từ Server chính

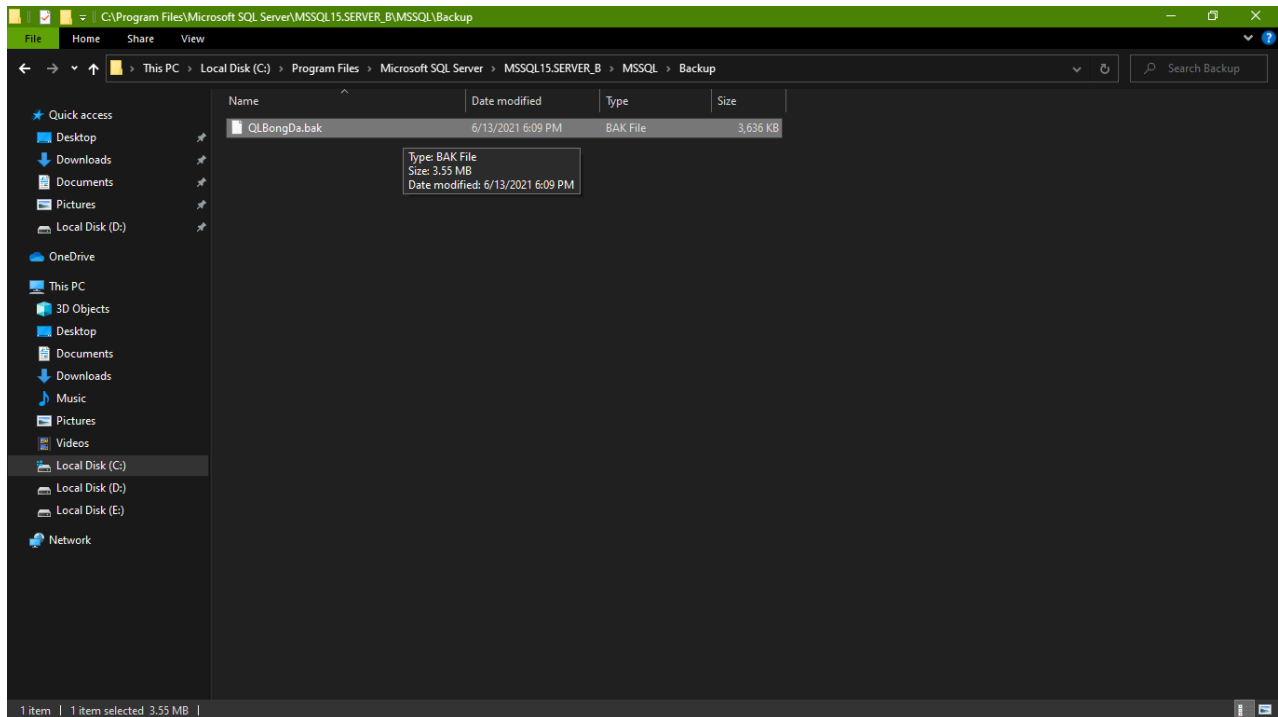
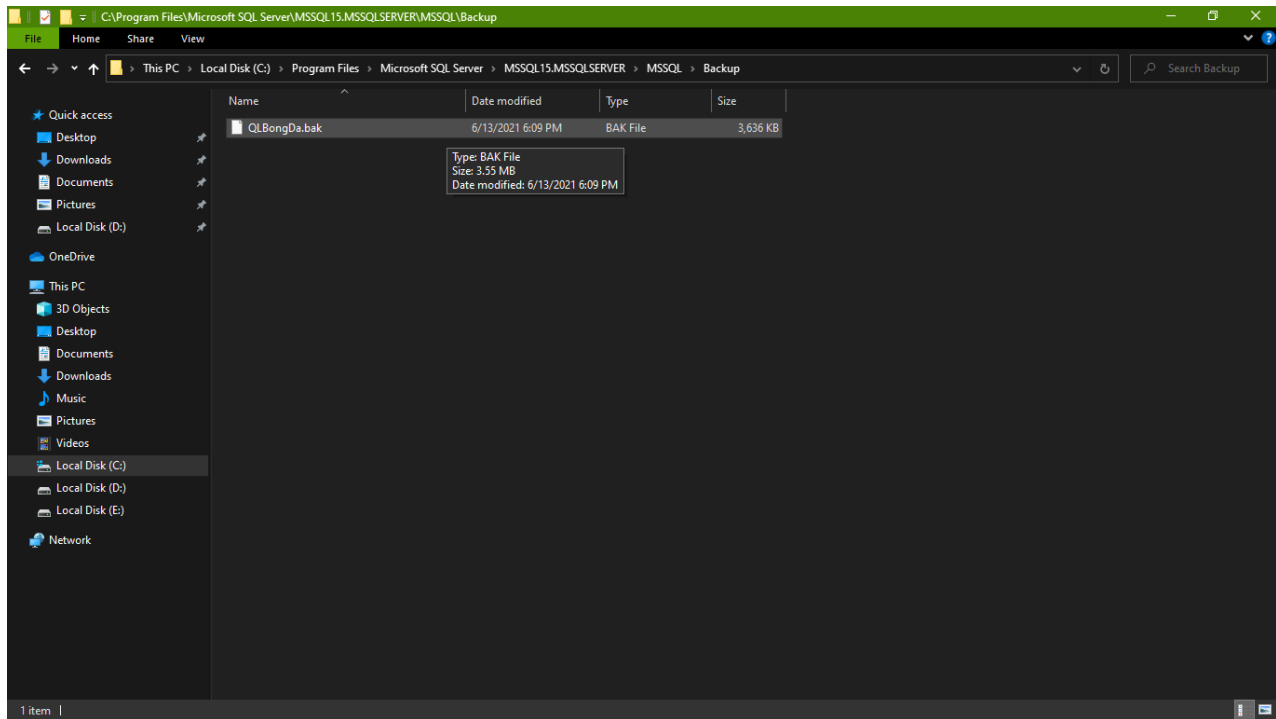


III.2. Backup – Restore

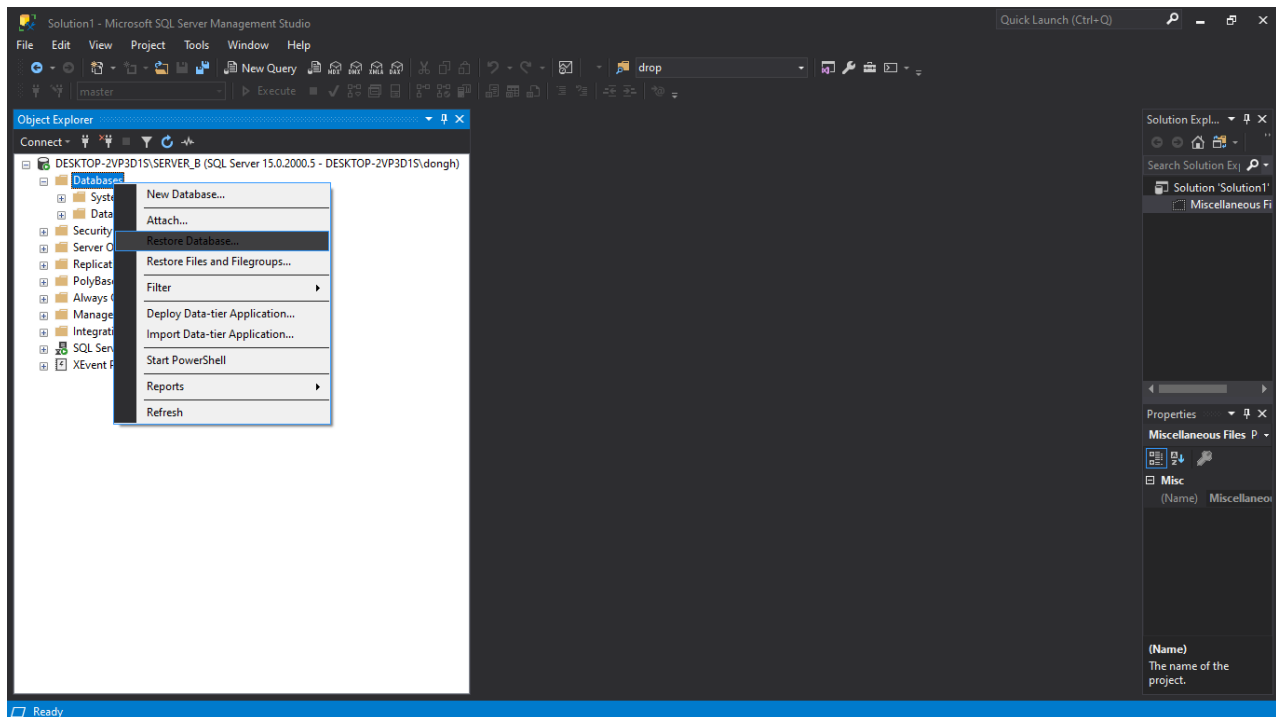
- Tại Server chính tiến hành tạo file Backup



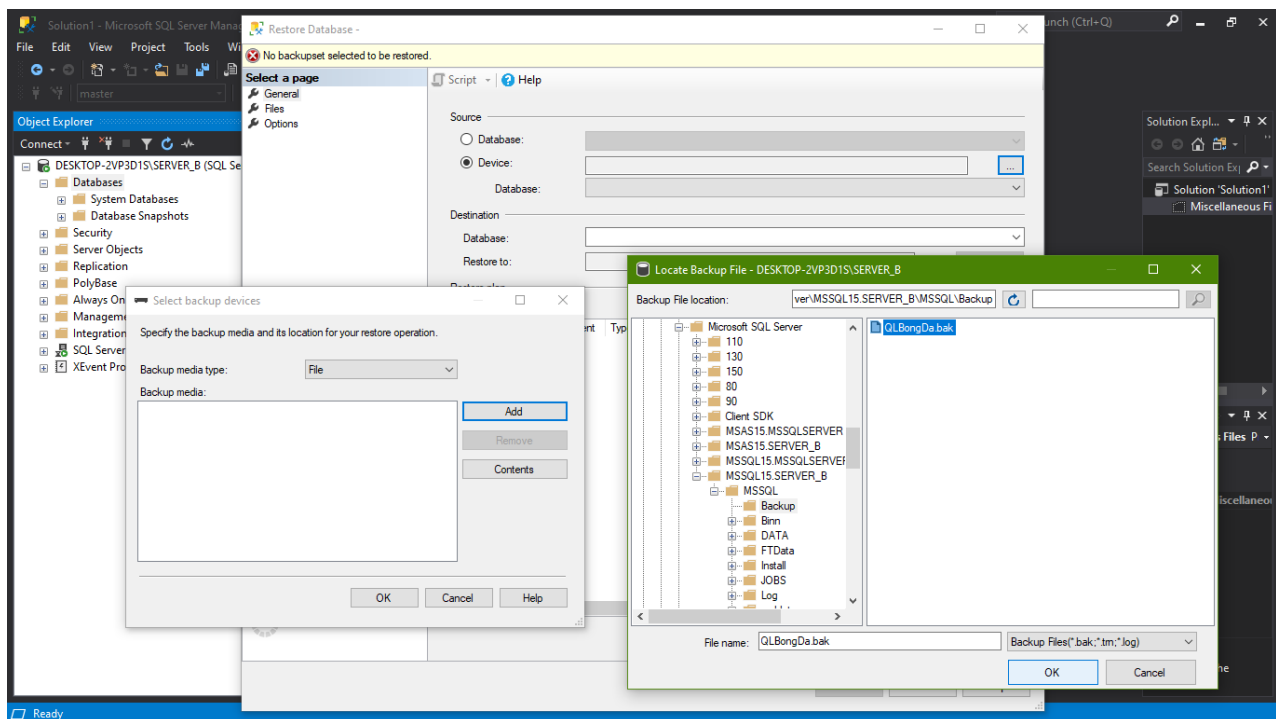
- Copy file Backup từ folder Server chính qua folder Server_B

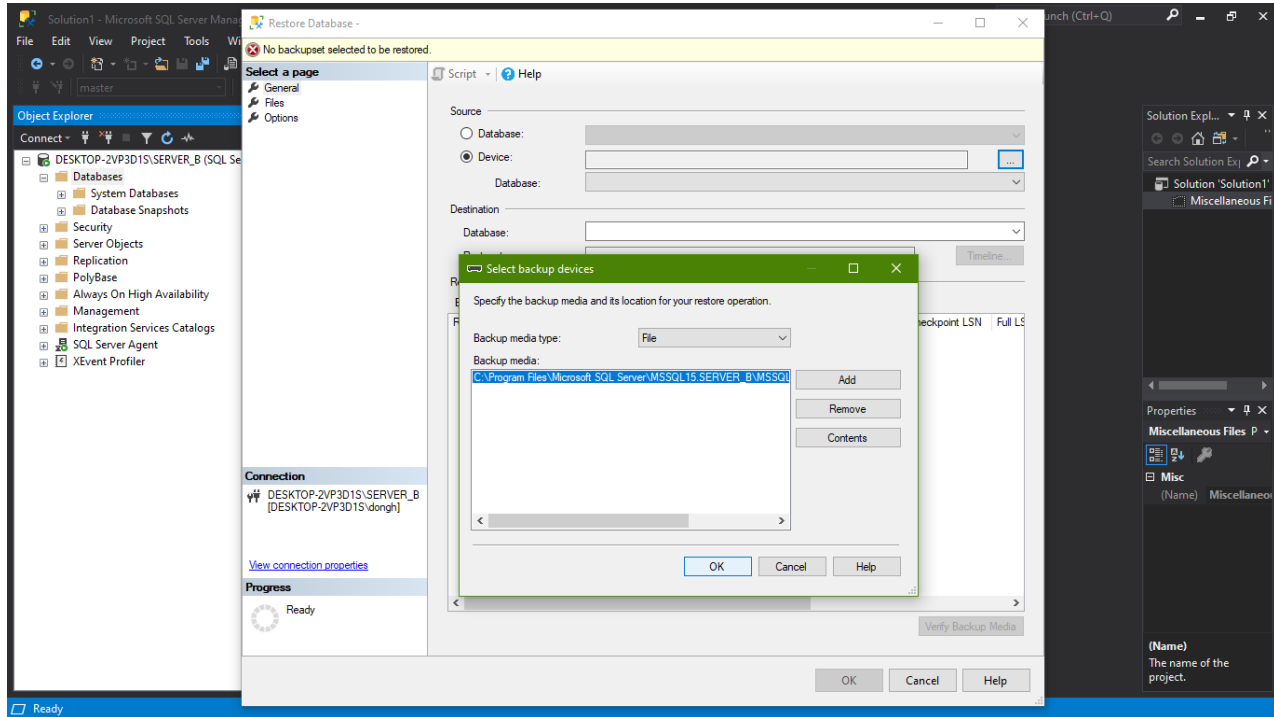


- Tiến hành Restore tại Server_B

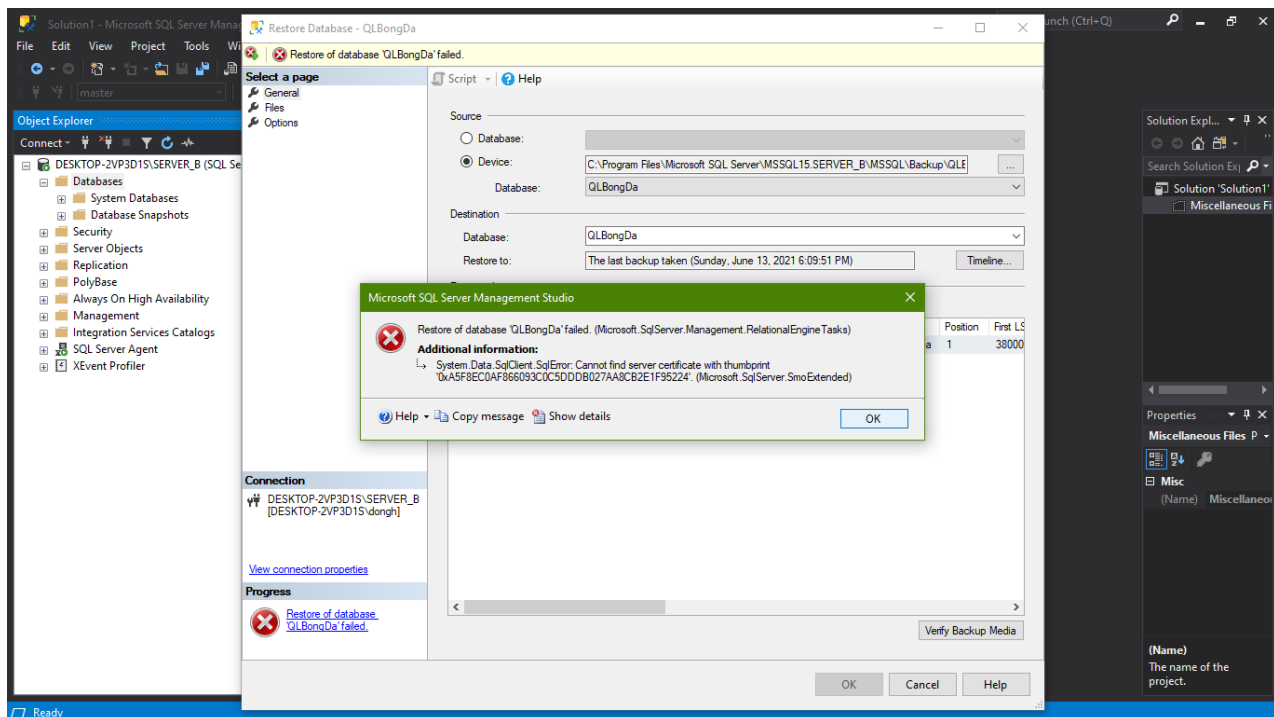


- Chọn file Backup



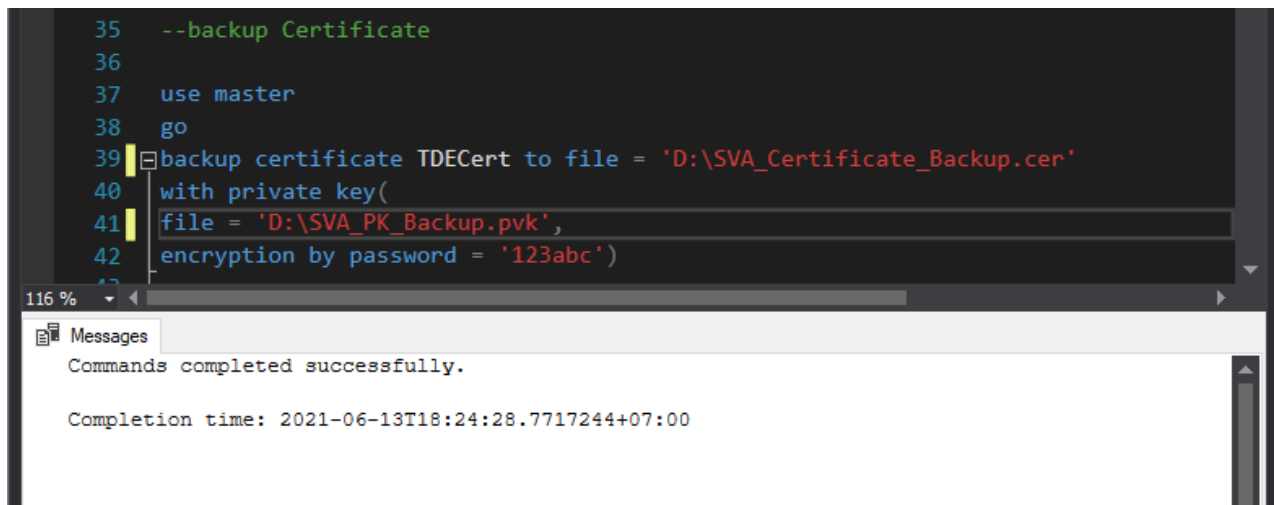


- Restore thất bại do không có Certificate và Key mã hóa Database từ Server chính



III.3. Giải pháp

- Ta cần phải backup lại Certificate dùng để mã hóa dữ liệu ở Server chính và khôi phục lại Certificate đó để giải mã dữ liệu ở Server kia. Sau khi Restore thành công Certificate thì Database QLBongDa có thể được Attach và Restore lại như bình thường
 - o Backup lại Certificate ở server ban đầu



```
35  --backup Certificate
36
37  use master
38  go
39  backup certificate TDECert to file = 'D:\SVA_Certificate_Backup.cer'
40  with private key(
41  file = 'D:\SVA_PK_Backup.pvk',
42  encryption by password = '123abc')
```

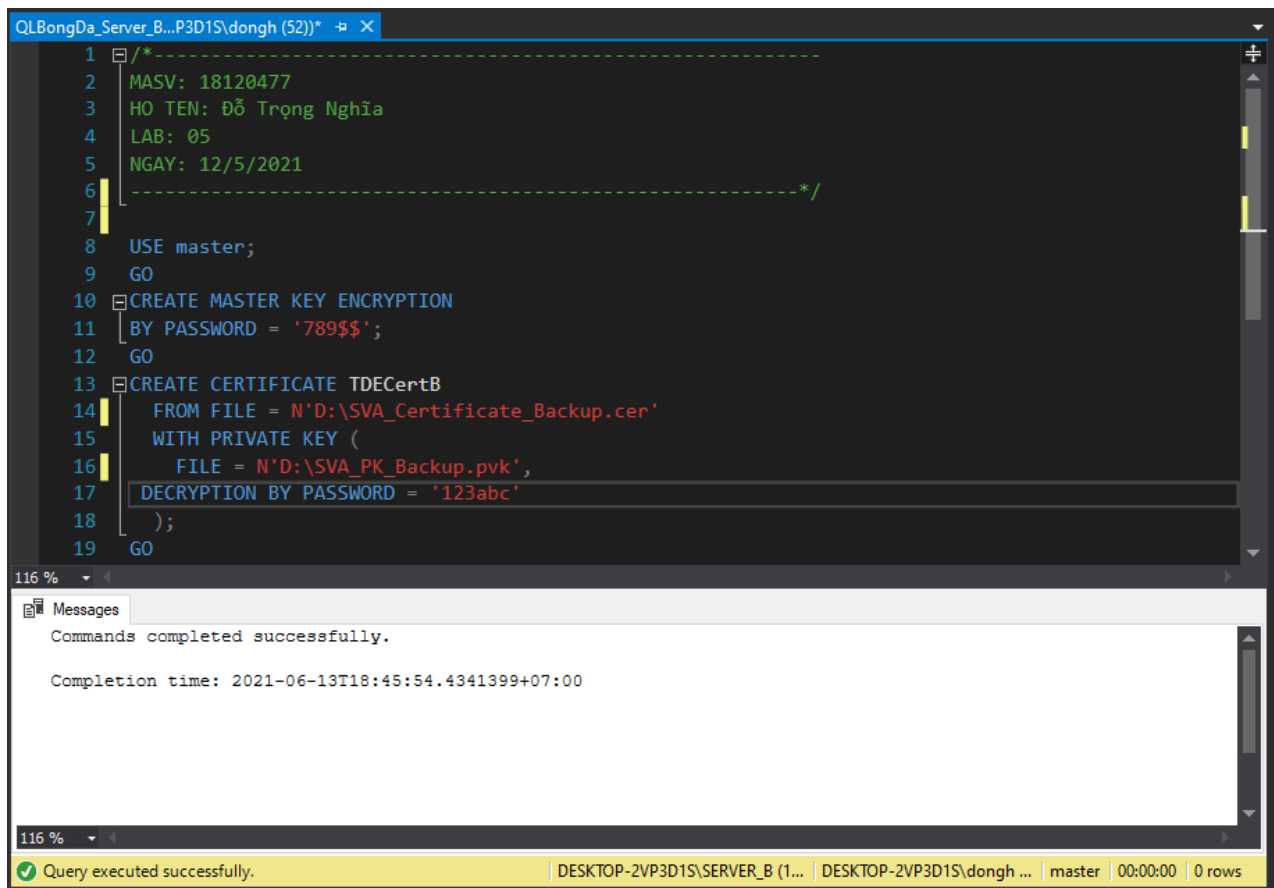
116 %

Messages

Commands completed successfully.

Completion time: 2021-06-13T18:24:28.7717244+07:00

- Khôi phục lại Certificate ở server ban đầu từ file back up, file private key và phải mật khẩu dùng để mã hóa Certificate đó



The screenshot shows a SQL Server Enterprise Manager interface. The top pane displays a T-SQL script with the following content:

```
1  /*-----*/
2  MASV: 18120477
3  HỌ TÊN: Đỗ Trọng Nghĩa
4  LAB: 05
5  NGÀY: 12/5/2021
6  -----*/
7
8  USE master;
9  GO
10 CREATE MASTER KEY ENCRYPTION
11 BY PASSWORD = '789$$';
12 GO
13 CREATE CERTIFICATE TDECertB
14 FROM FILE = N'D:\SVA_Certificate_Backup.cer'
15 WITH PRIVATE KEY (
16 FILE = N'D:\SVA_PK_Backup.pvk',
17 DECRYPTION BY PASSWORD = '123abc'
18 );
19 GO
```

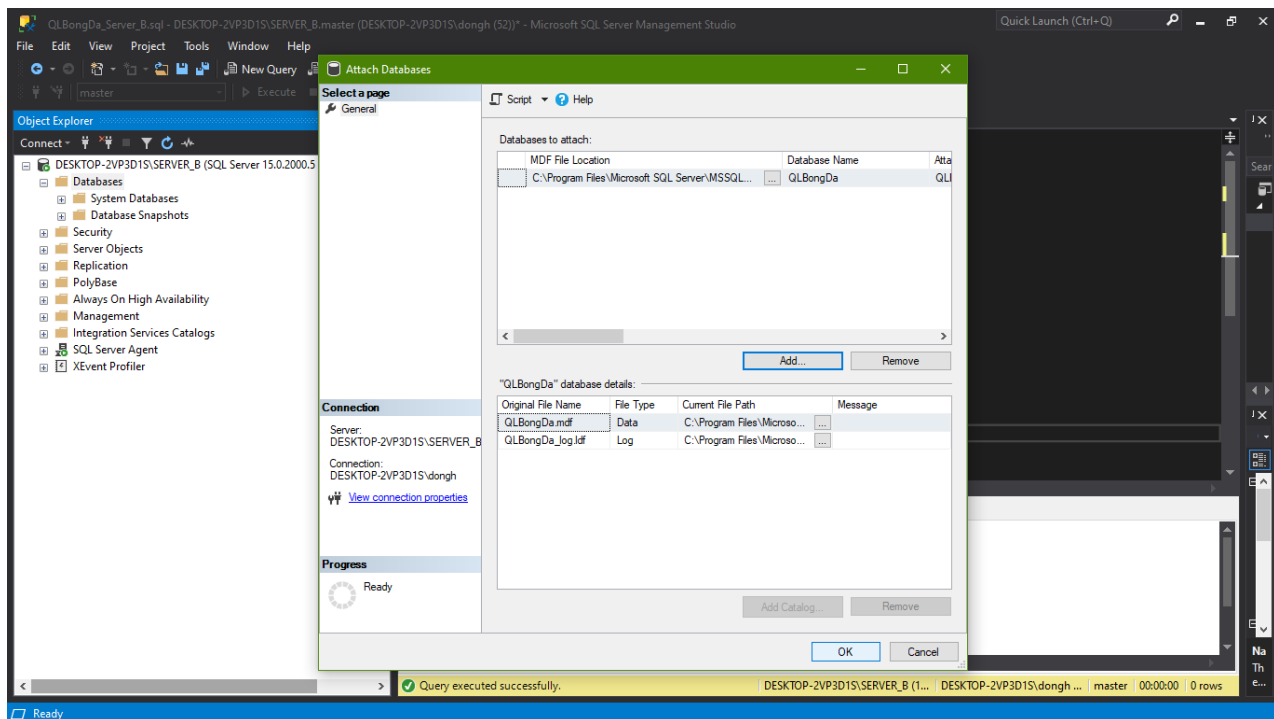
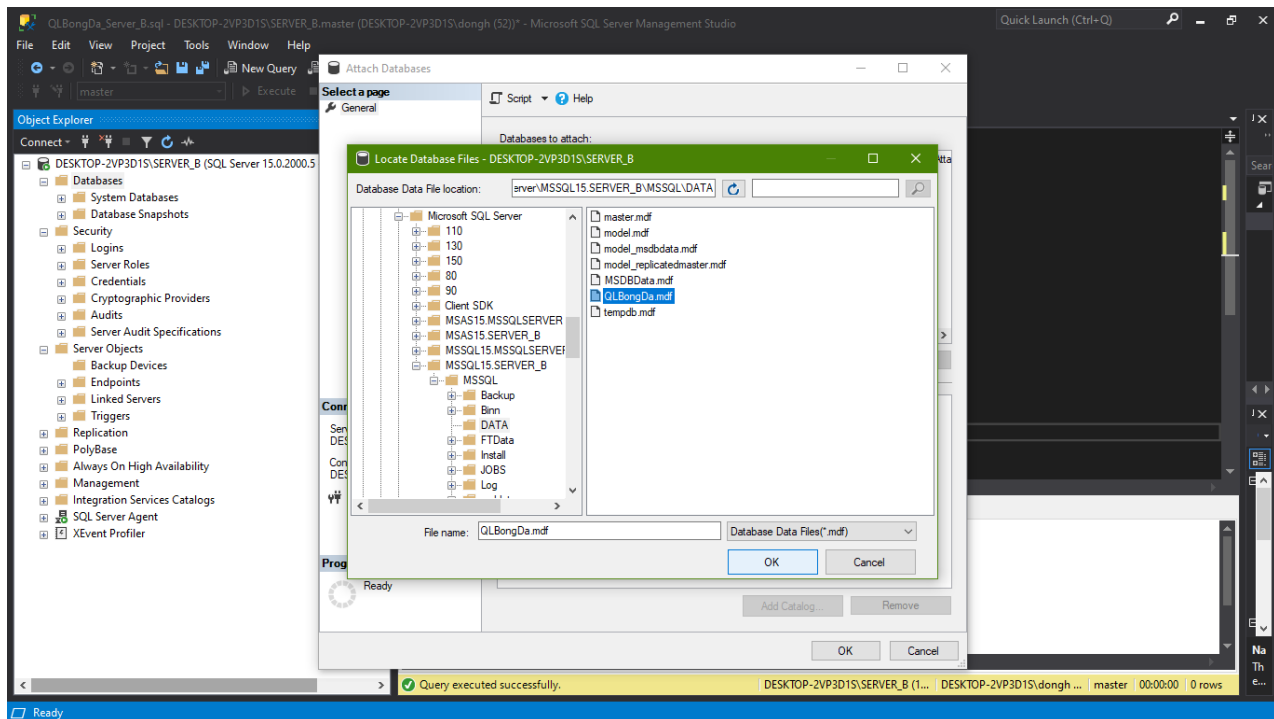
The bottom pane shows the Messages window with the following text:

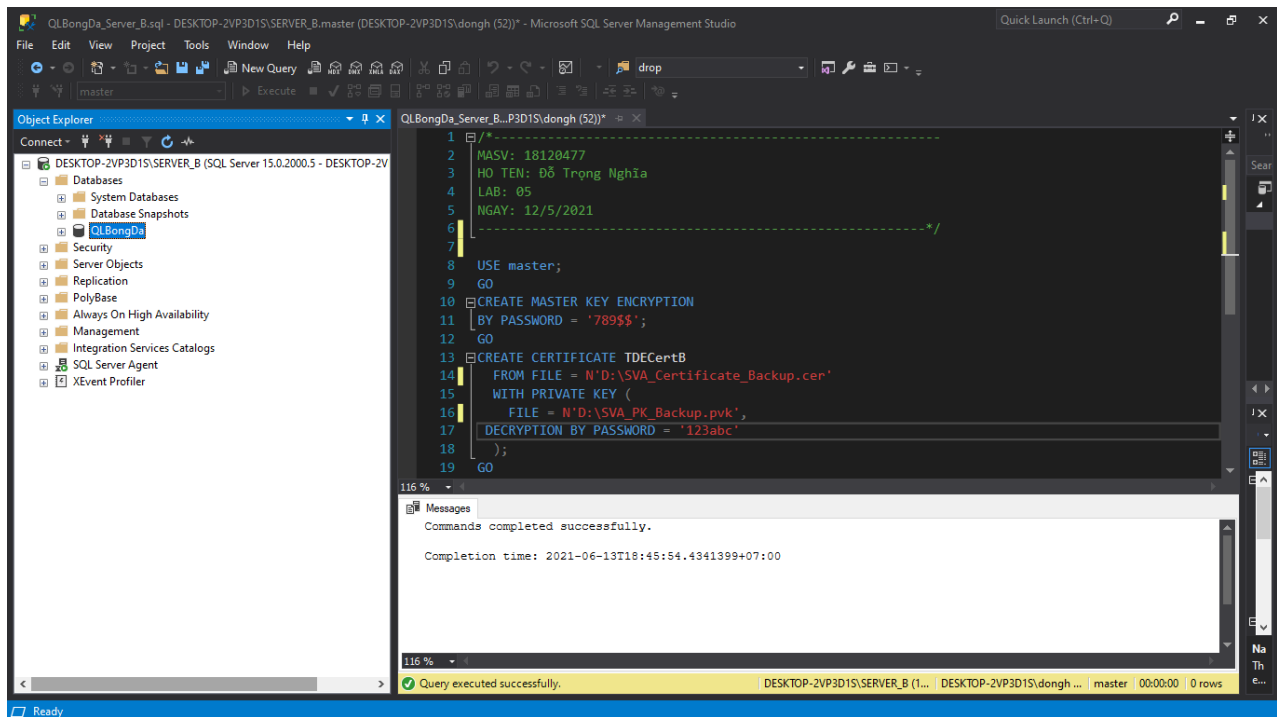
```
Commands completed successfully.
Completion time: 2021-06-13T18:45:54.4341399+07:00
```

The status bar at the bottom indicates: Query executed successfully. | DESKTOP-2VP3D1S\SERVER_B (1... | DESKTOP-2VP3D1S\dongh ... | master | 00:00:00 | 0 rows

- Sau đó Detach và Restore lại ở Server_B để kiểm tra

- Detach Database ở Server_B thành công





- Restore Database thành công

