**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**

**Họ tên: VÕ PHI HÙNG MÔN: AN TOÀN ỨNG DỤNG WEB VÀ CSDL**

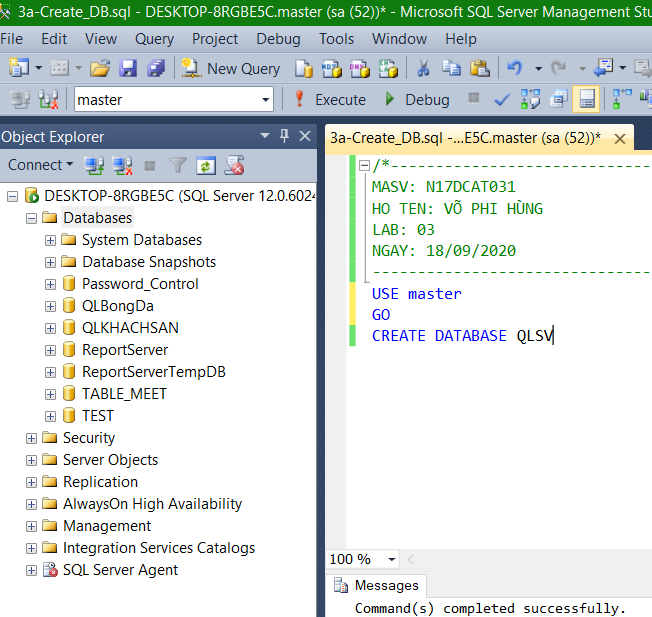
**Mã lớp: D17CQAT01-N**

**MSSV: N17DCAT031**

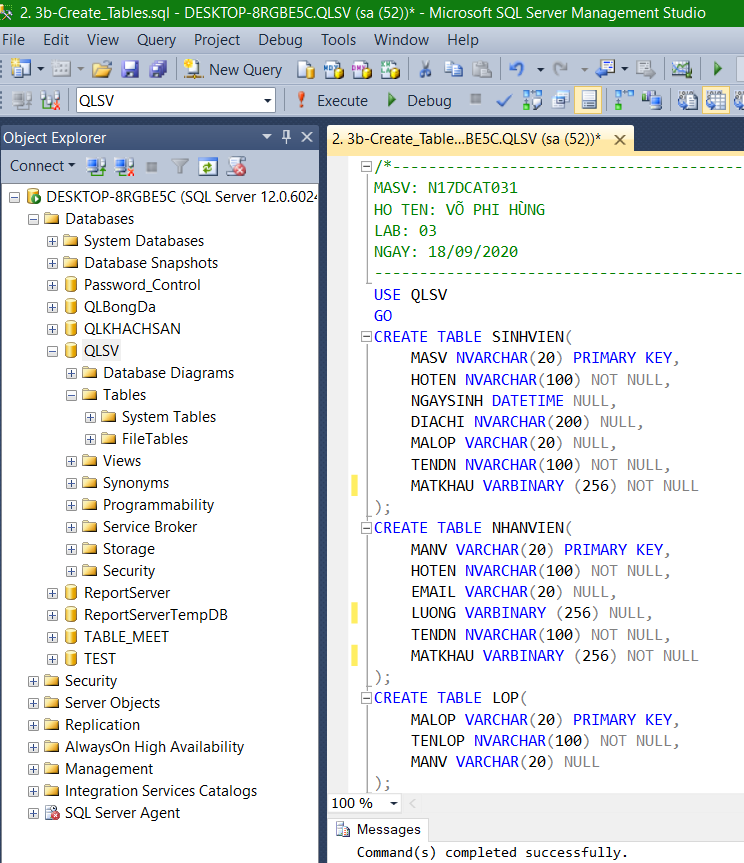
**LAB 3**

**3. Yêu cầu thực hành.**

a) Viết script tạo Database có tên QLSV\_DG.

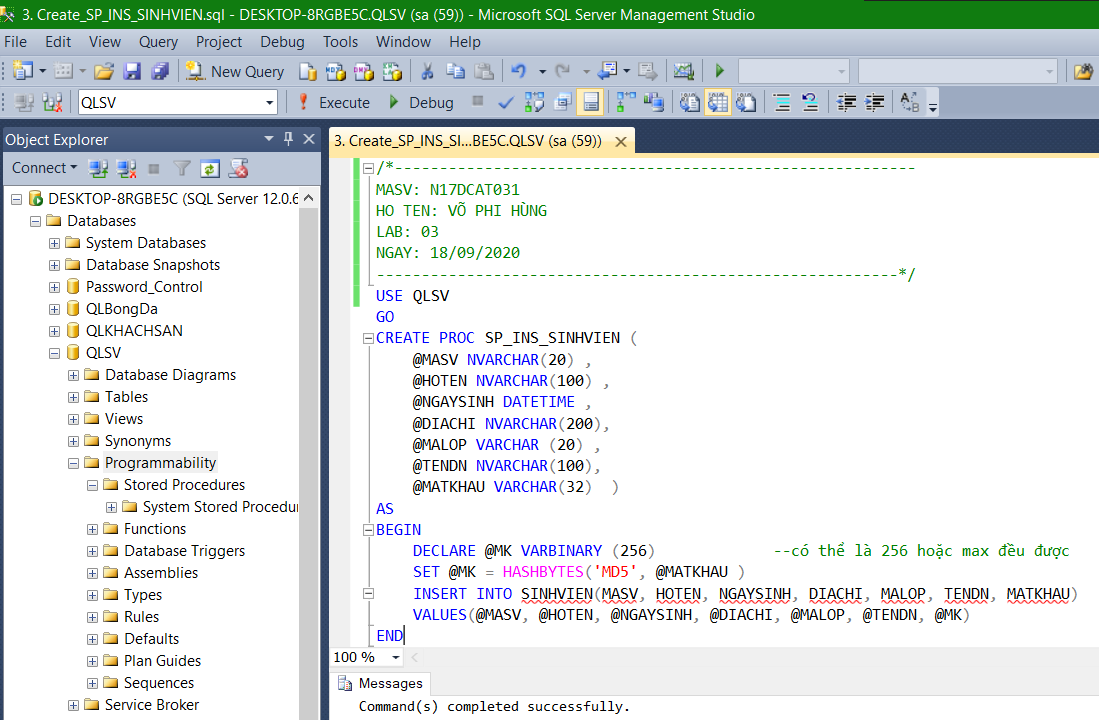


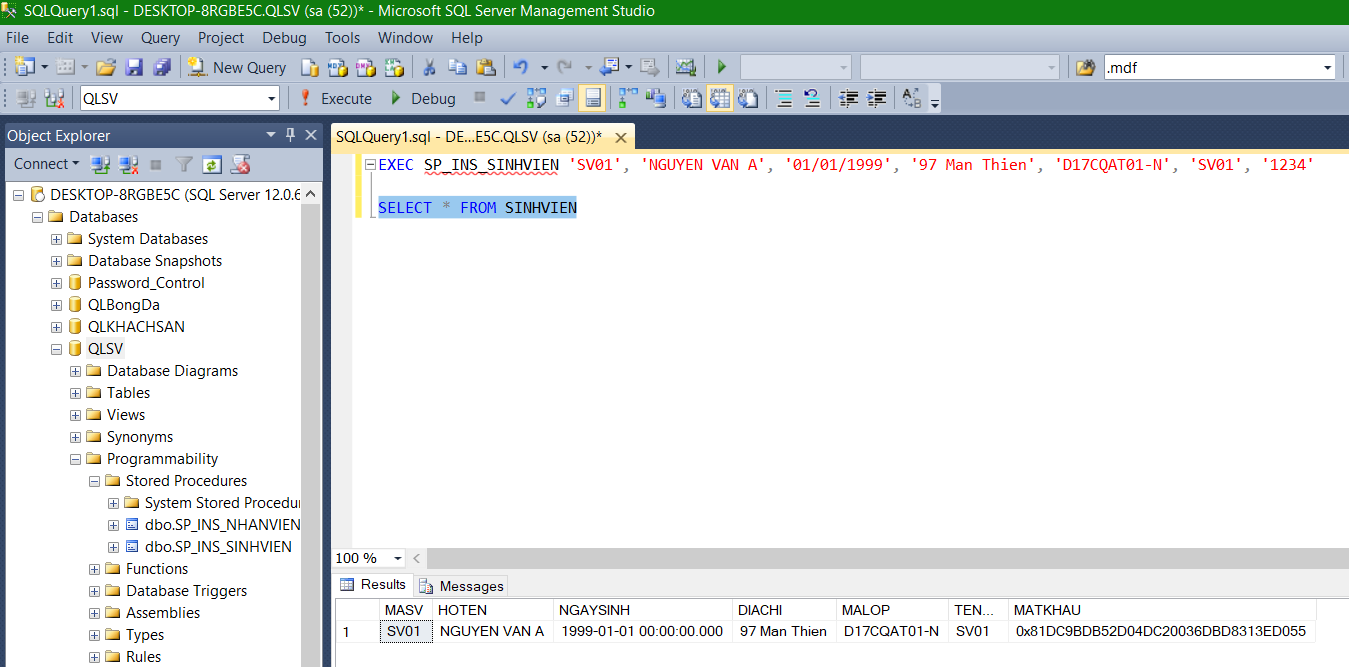
b) Viết script tạo mới các Table **SINHVIEN**, **NHANVIEN**, **LOP**.



**c) Viết các Stored procedure sau:**

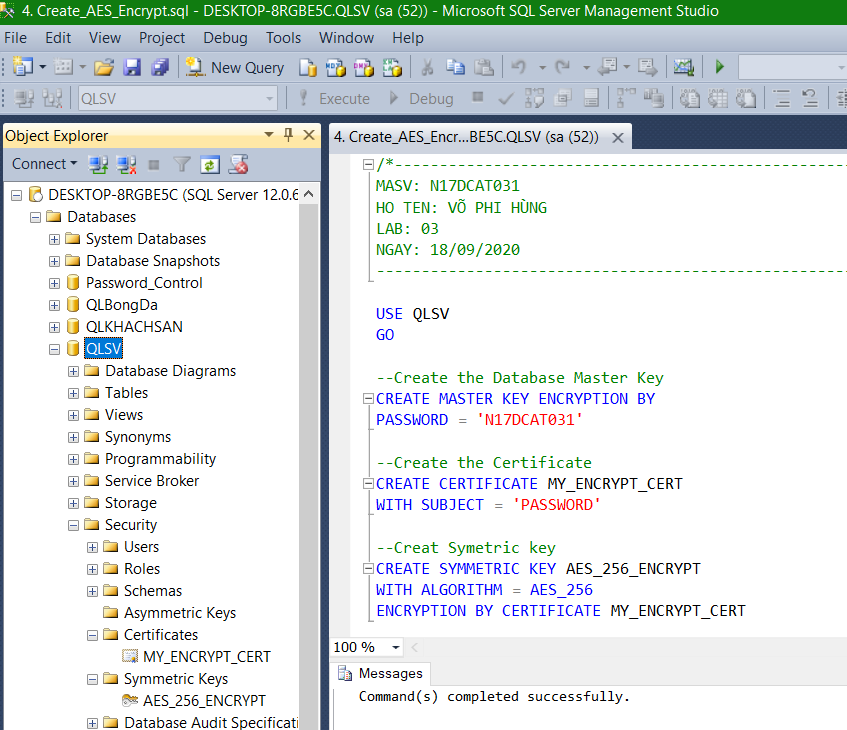
**i) Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng MD5.**



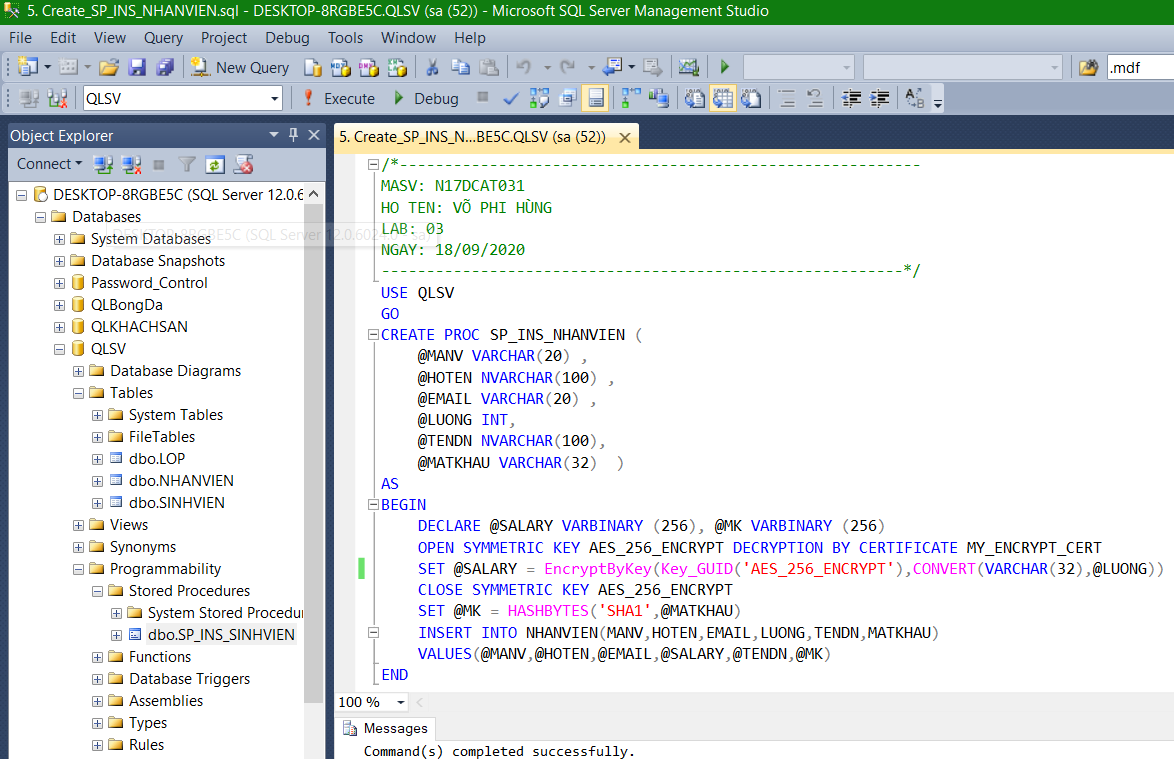


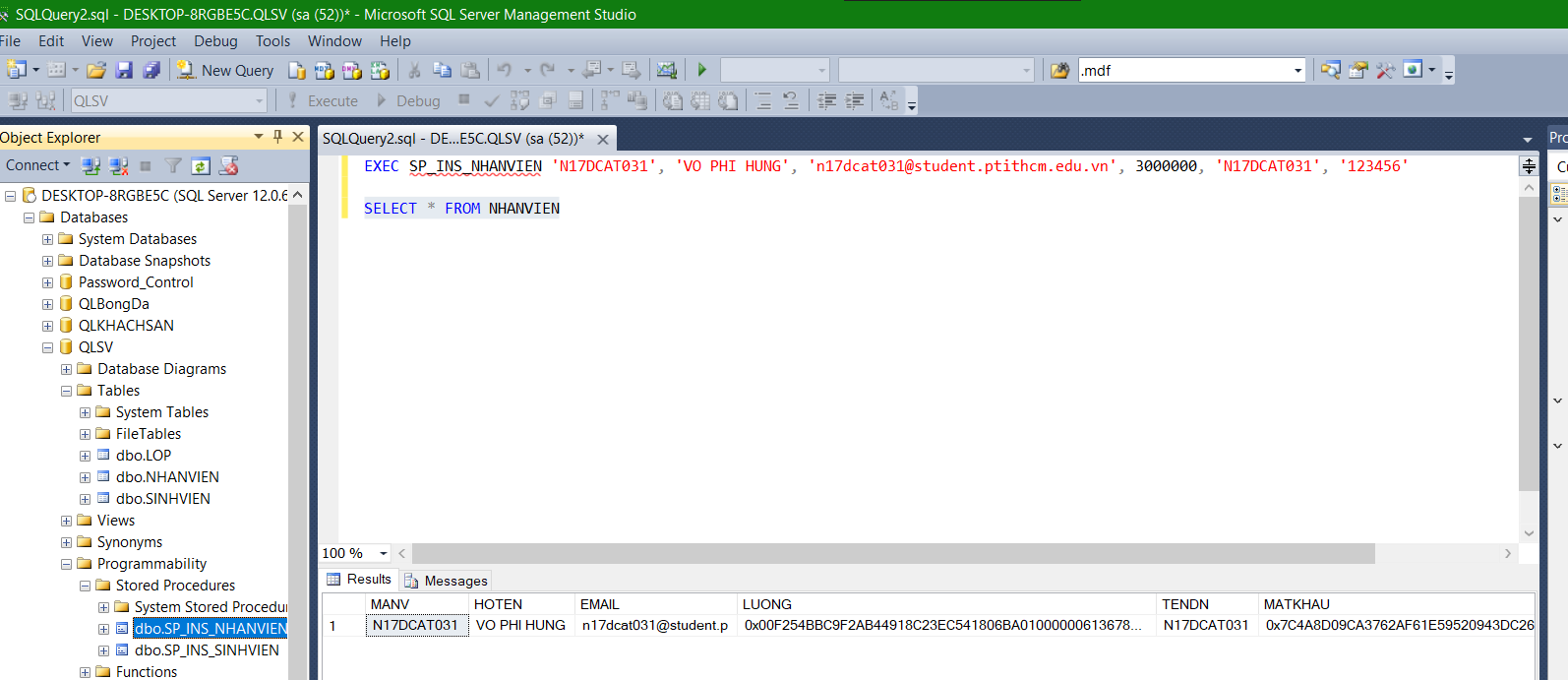
**ii) Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng SHA1 và thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán AES 256, với khóa mã hóa là mã số của sinh viên thực hiện bài Lab này – ‘N17DCAT031’.**

* Trước tiên bạn cần tạo **Master Key**, **Certificate** và **Symmetric Key** cho DB **QLSV**. **Symmetric key** **AES\_256\_ENCRYPT** này được dùng để mã hóa dữ liệu dựa trên chứng chỉ **MY\_ENCRYPT\_CERT** lấy **PASSWORD** là ‘**N17DCAT031**’.

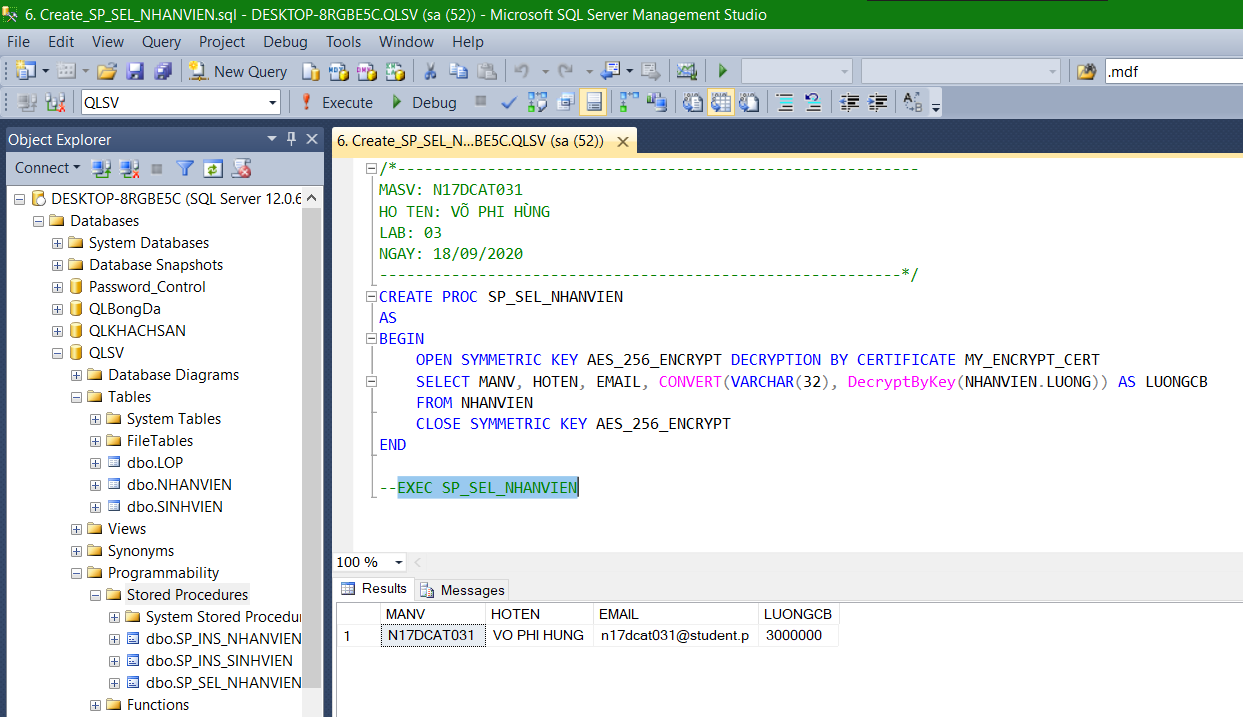


* Tạo **SP\_INS\_NHANVIEN**:





**iii)** Stored dùng để **truy vấn dữ liệu** nhân viên (**NHANVIEN**):



**d) Viết màn hình quản lý đăng nhập hệ thống (sử dụng JAVA), cho phép nhập vào tên đăng nhập và mật khẩu (giả sử tên đăng nhập của sinh viên và nhân viên là duy nhất, nghĩa là tên đăng nhập của tất cả các sinh viên và tất cả nhân viên là khác nhau).**

**\*\*Ghi chú 1: Source code hình dưới có trong Project “ATWEB\_CSDL” đính kèm:**

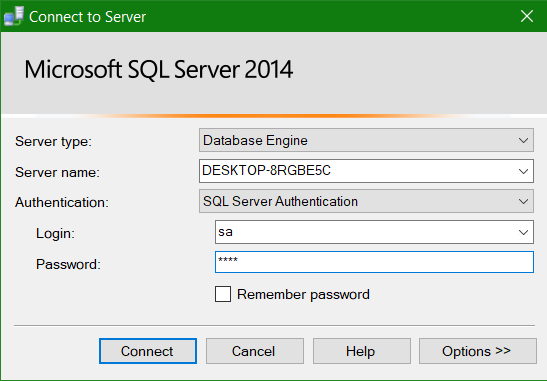
* Tài khoản login: SINHVIEN: **SV01** – **1234**; NHANVIEN: **N17DCAT031** – **123456**
* Hai tài khoản trên chạy tốt với cơ sở dữ liệu “**QLSV**” đính kèm.

**\*\*Ghi chú 2: Trong hình dưới, code dùng lệnh truy vấn cơ sở dữ liệu chưa được bảo mật tốt, vì khi attacker có được source code của chương trình sẽ biết được kiểu mã hóa của chúng ta là gì, ít tốn thời gian hơn để tìm ra kiểu mã hóa.**

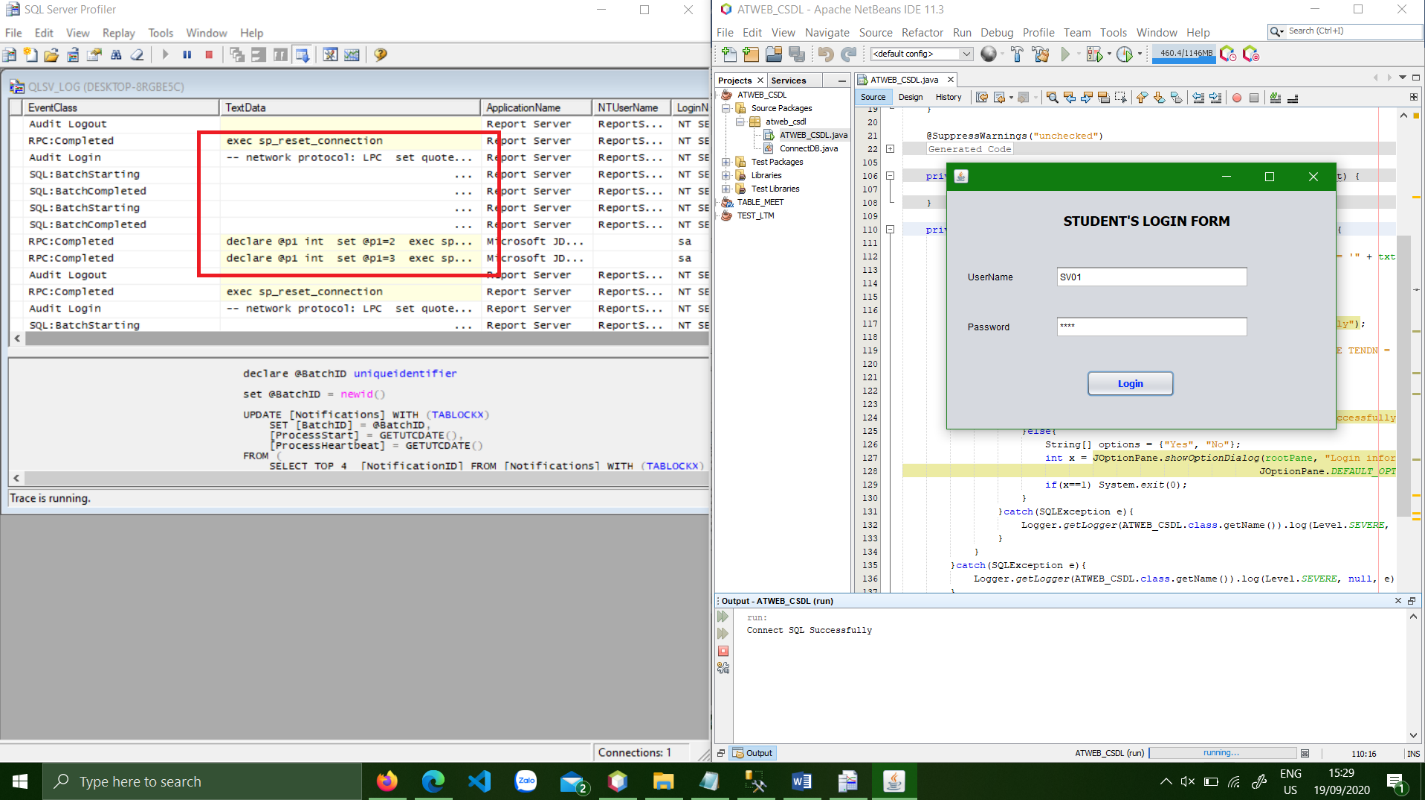


**e) Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập từ màn hình quản lý đăng nhập trên, nhận xét.**

**i) Login SQL “sa”:**

****

**ii) Sau khi tạo file .trc bên màn trình quản lý SQL Profiler, tiến hành đăng nhập vào SQL Server bằng chương trình đăng nhập của Java đã tạo ở trên, nhận thấy kết quả, chưa tính đến việc đăng nhập tài khoản đã đúng hay chưa, mỗi lần ta bấm nút Login, bên màn hình Profiler sẽ in ra các dòng trong khung đỏ, đó là các ghi nhận khi ta thực thi bất kỳ thao tác gì trên CSDL.**

****