

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
ĐẠI HỌC KHOA HỌC TỰ NHIÊN TPHCM

-----0-----

BÁO CÁO ĐỒ ÁN

Tên Đồ Án: Crack phần mềm

Đề: 1



Sinh viên thực hiện: Nguyễn Hữu Tú – 1612766

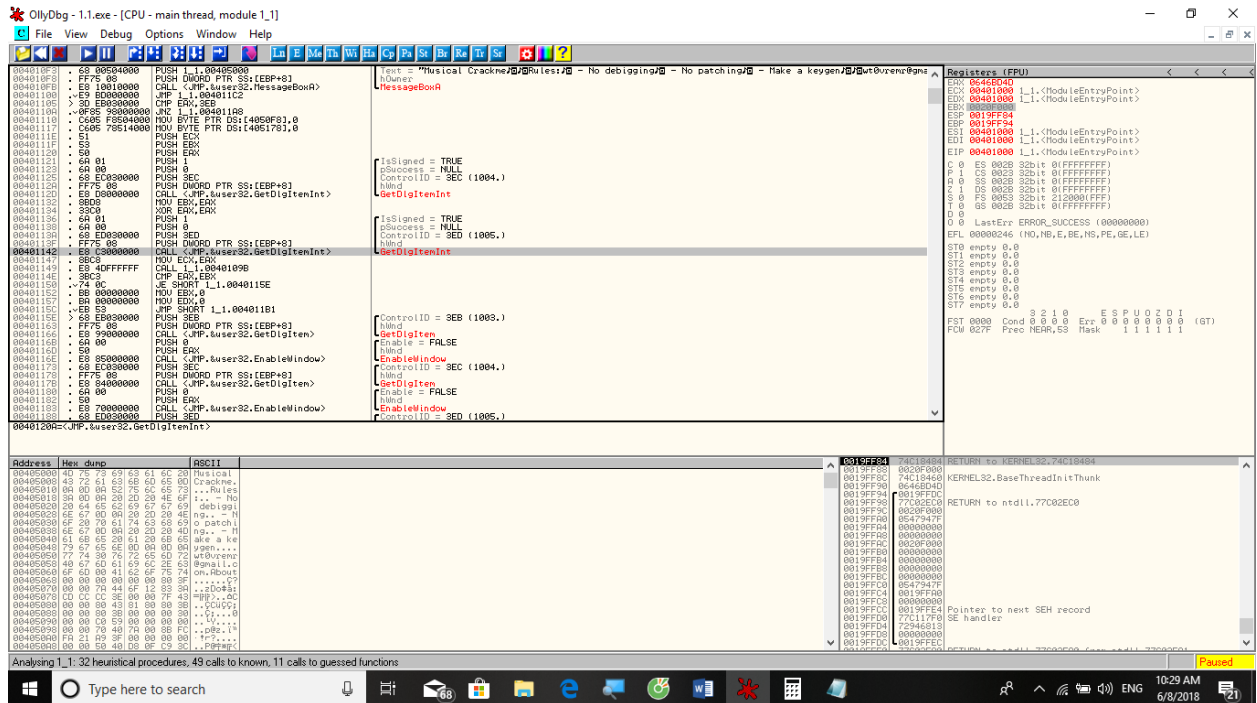
Nguyễn Anh Tuấn – 1612778

- Dòng 0040112D là dòng lấy Personal ID(chỉ nhập số, không quá 4 số)

The screenshot shows the OllyDbg interface with the following details:

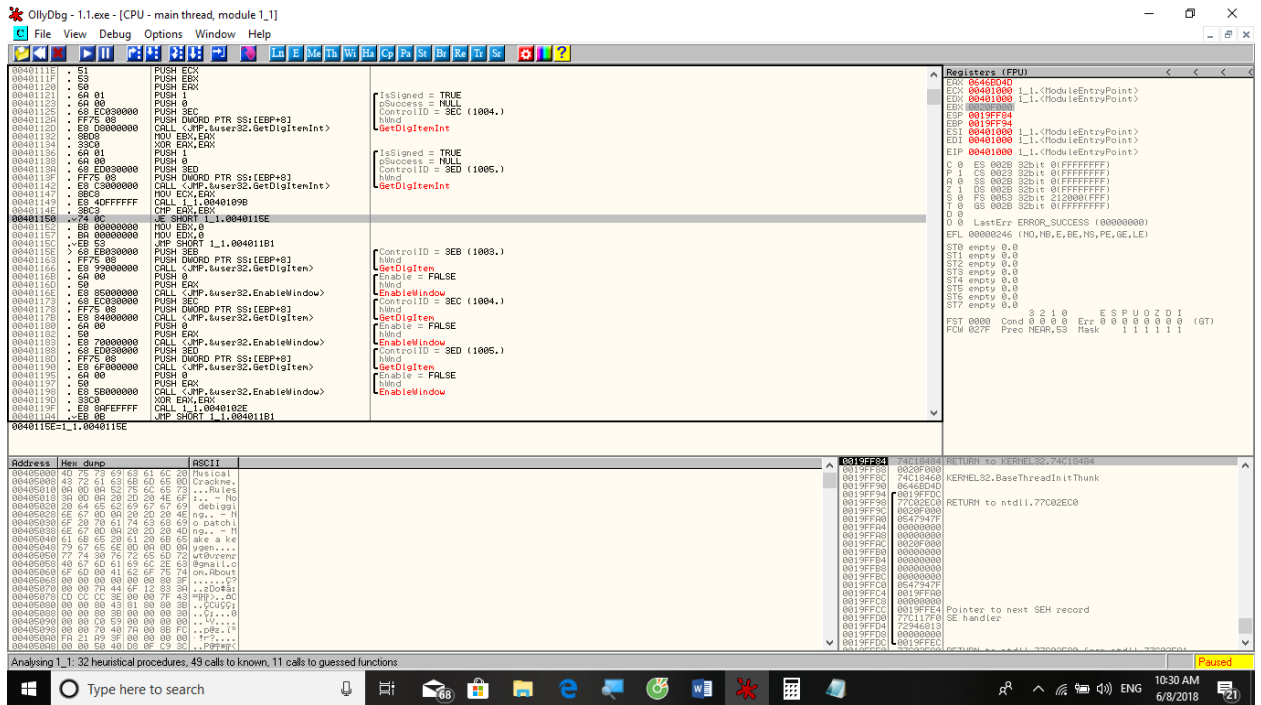
- Assembly Window:** Displays assembly code for a function. Key instructions include:
 - `00401000 .EIP 00401000: PUSH EAX`
 - `00401001 .EIP 00401001: CALL [EIP, user32.MessageBox]`
 - `00401002 .EIP 00401002: CMP EAX, 0`
 - `00401003 .EIP 00401003: JZ 00401008`
 - `00401004 .EIP 00401004: MOV EAX, 0`
 - `00401005 .EIP 00401005: MOV EAX, 0`
 - `00401006 .EIP 00401006: MOV EAX, 0`
 - `00401007 .EIP 00401007: MOV EAX, 0`
 - `00401008 .EIP 00401008: MOV EAX, 0`
 - `00401009 .EIP 00401009: MOV EAX, 0`
 - `00401010 .EIP 00401010: MOV EAX, 0`
 - `00401011 .EIP 00401011: MOV EAX, 0`
 - `00401012 .EIP 00401012: MOV EAX, 0`
 - `00401013 .EIP 00401013: MOV EAX, 0`
 - `00401014 .EIP 00401014: MOV EAX, 0`
 - `00401015 .EIP 00401015: MOV EAX, 0`
 - `00401016 .EIP 00401016: MOV EAX, 0`
 - `00401017 .EIP 00401017: MOV EAX, 0`
 - `00401018 .EIP 00401018: MOV EAX, 0`
 - `00401019 .EIP 00401019: MOV EAX, 0`
 - `00401020 .EIP 00401020: MOV EAX, 0`
 - `00401021 .EIP 00401021: MOV EAX, 0`
 - `00401022 .EIP 00401022: MOV EAX, 0`
 - `00401023 .EIP 00401023: MOV EAX, 0`
 - `00401024 .EIP 00401024: MOV EAX, 0`
 - `00401025 .EIP 00401025: MOV EAX, 0`
 - `00401026 .EIP 00401026: MOV EAX, 0`
 - `00401027 .EIP 00401027: MOV EAX, 0`
 - `00401028 .EIP 00401028: MOV EAX, 0`
 - `00401029 .EIP 00401029: MOV EAX, 0`
 - `00401030 .EIP 00401030: MOV EAX, 0`
 - `00401031 .EIP 00401031: MOV EAX, 0`
 - `00401032 .EIP 00401032: MOV EAX, 0`
 - `00401033 .EIP 00401033: MOV EAX, 0`
 - `00401034 .EIP 00401034: MOV EAX, 0`
 - `00401035 .EIP 00401035: MOV EAX, 0`
 - `00401036 .EIP 00401036: MOV EAX, 0`
 - `00401037 .EIP 00401037: MOV EAX, 0`
 - `00401038 .EIP 00401038: MOV EAX, 0`
 - `00401039 .EIP 00401039: MOV EAX, 0`
 - `00401040 .EIP 00401040: MOV EAX, 0`
 - `00401041 .EIP 00401041: MOV EAX, 0`
 - `00401042 .EIP 00401042: MOV EAX, 0`
 - `00401043 .EIP 00401043: MOV EAX, 0`
 - `00401044 .EIP 00401044: MOV EAX, 0`
 - `00401045 .EIP 00401045: MOV EAX, 0`
 - `00401046 .EIP 00401046: MOV EAX, 0`
 - `00401047 .EIP 00401047: MOV EAX, 0`
 - `00401048 .EIP 00401048: MOV EAX, 0`
 - `00401049 .EIP 00401049: MOV EAX, 0`
 - `00401050 .EIP 00401050: MOV EAX, 0`
 - `00401051 .EIP 00401051: MOV EAX, 0`
 - `00401052 .EIP 00401052: MOV EAX, 0`
 - `00401053 .EIP 00401053: MOV EAX, 0`
 - `00401054 .EIP 00401054: MOV EAX, 0`
 - `00401055 .EIP 00401055: MOV EAX, 0`
 - `00401056 .EIP 00401056: MOV EAX, 0`
 - `00401057 .EIP 00401057: MOV EAX, 0`
 - `00401058 .EIP 00401058: MOV EAX, 0`
 - `00401059 .EIP 00401059: MOV EAX, 0`
 - `00401060 .EIP 00401060: MOV EAX, 0`
 - `00401061 .EIP 00401061: MOV EAX, 0`
 - `00401062 .EIP 00401062: MOV EAX, 0`
 - `00401063 .EIP 00401063: MOV EAX, 0`
 - `00401064 .EIP 00401064: MOV EAX, 0`
 - `00401065 .EIP 00401065: MOV EAX, 0`
 - `00401066 .EIP 00401066: MOV EAX, 0`
 - `00401067 .EIP 00401067: MOV EAX, 0`
 - `00401068 .EIP 00401068: MOV EAX, 0`
 - `00401069 .EIP 00401069: MOV EAX, 0`
 - `00401070 .EIP 00401070: MOV EAX, 0`
 - `00401071 .EIP 00401071: MOV EAX, 0`
 - `00401072 .EIP 00401072: MOV EAX, 0`
 - `00401073 .EIP 00401073: MOV EAX, 0`
 - `00401074 .EIP 00401074: MOV EAX, 0`
 - `00401075 .EIP 00401075: MOV EAX, 0`
 - `00401076 .EIP 00401076: MOV EAX, 0`
 - `00401077 .EIP 00401077: MOV EAX, 0`
 - `00401078 .EIP 00401078: MOV EAX, 0`
 - `00401079 .EIP 00401079: MOV EAX, 0`
 - `00401080 .EIP 00401080: MOV EAX, 0`
 - `00401081 .EIP 00401081: MOV EAX, 0`
 - `00401082 .EIP 00401082: MOV EAX, 0`
 - `00401083 .EIP 00401083: MOV EAX, 0`
 - `00401084 .EIP 00401084: MOV EAX, 0`
 - `00401085 .EIP 00401085: MOV EAX, 0`
 - `00401086 .EIP 00401086: MOV EAX, 0`
 - `00401087 .EIP 00401087: MOV EAX, 0`
 - `00401088 .EIP 00401088: MOV EAX, 0`
 - `00401089 .EIP 00401089: MOV EAX, 0`
 - `00401090 .EIP 00401090: MOV EAX, 0`
 - `00401091 .EIP 00401091: MOV EAX, 0`
 - `00401092 .EIP 00401092: MOV EAX, 0`
 - `00401093 .EIP 00401093: MOV EAX, 0`
 - `00401094 .EIP 00401094: MOV EAX, 0`
 - `00401095 .EIP 00401095: MOV EAX, 0`
 - `00401096 .EIP 00401096: MOV EAX, 0`
 - `00401097 .EIP 00401097: MOV EAX, 0`
 - `00401098 .EIP 00401098: MOV EAX, 0`
 - `00401099 .EIP 00401099: MOV EAX, 0`
 - `00401100 .EIP 00401100: MOV EAX, 0`
 - `00401101 .EIP 00401101: MOV EAX, 0`
 - `00401102 .EIP 00401102: MOV EAX, 0`
 - `00401103 .EIP 00401103: MOV EAX, 0`
 - `00401104 .EIP 00401104: MOV EAX, 0`
 - `00401105 .EIP 00401105: MOV EAX, 0`

- Dòng 00401142 là dòng lấy số Serial (chỉ nhập số)

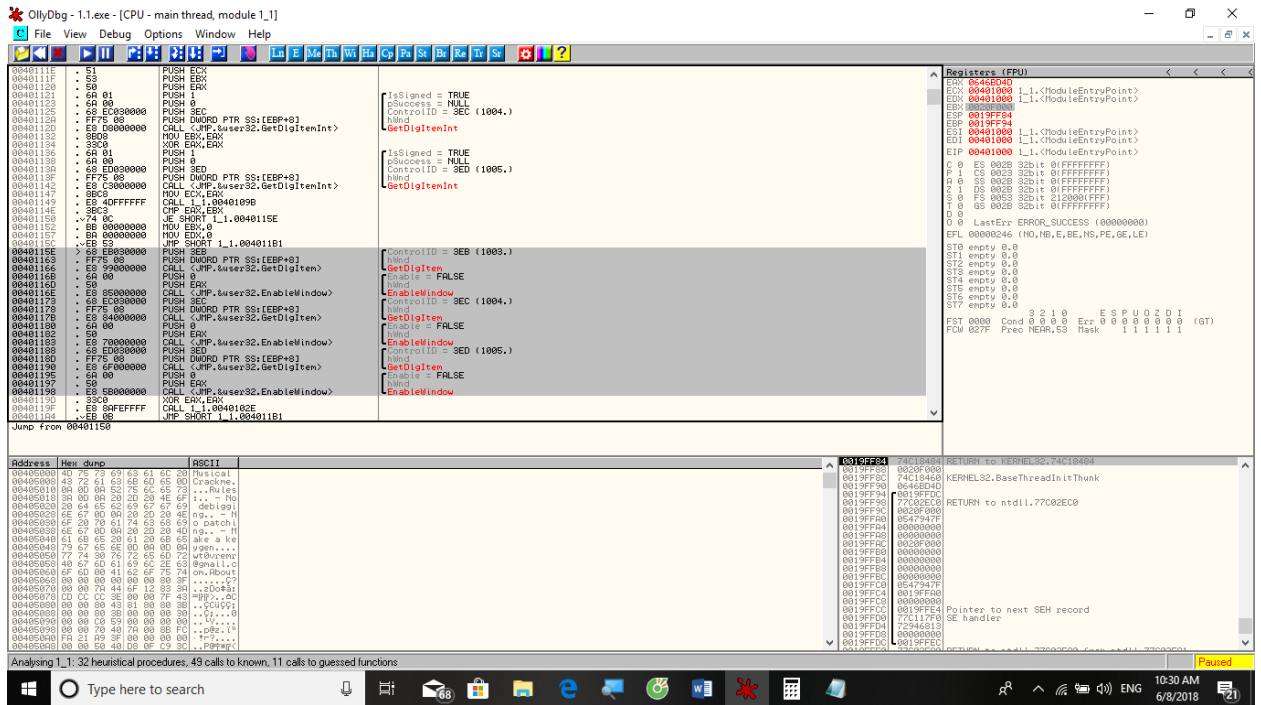


- Sau dòng 00401142 sẽ cập nhật giá trị thanh ghi EDX = 00000000
- Dòng 00401149 dùng để biến đổi giá trị ID đầu vào(được lưu trong EBX)

$$EBX = [(EBX + 4C + 1 + 38B) * 2 * (EDX + 3)] - 1$$



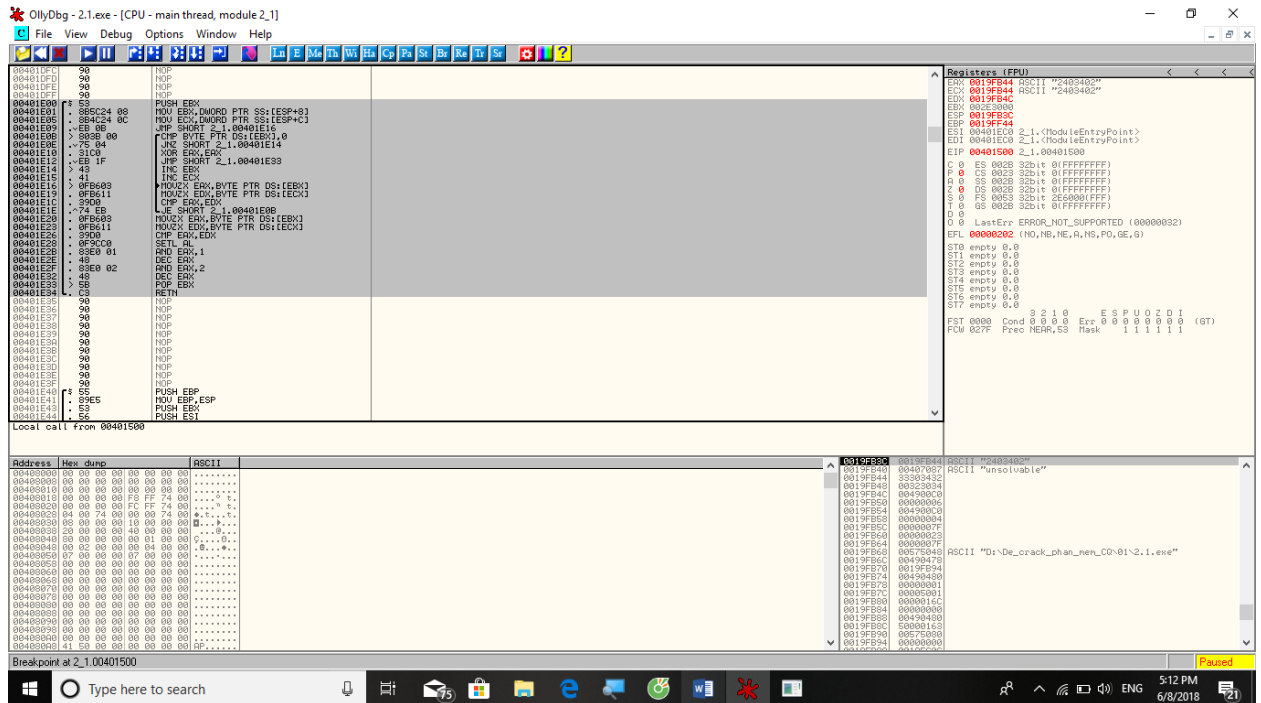
- Dòng 0040115E: Tôi được dòng lệnh này là có nghĩa serial và ID đã được chấp nhận và bắt đầu các câu lệnh xuất 1 đoạn nhạc ra.



- Key ví dụ: Id: 1024; serial: 12047

- Dòng 0040149F: Nhập username và lưu tại EAX
- Dòng 004014AC: đẩy username vào stack
- Dòng 004014AD: gọi hàm tính chiều dài username
- Dòng 004014B3 và 004014C5 để kiểm tra chiều dài nằm trong khoảng từ 5 đến 8, nếu không thì yêu cầu nhập lại.





- Dòng 00401507: Kiểm tra EAX có bằng 0 hay không, nếu có thì nhảy tới 0040152E để xuất thông báo sai và yêu cầu nhập lại; ngược lại thì không nhảy mà tiếp tục thực hiện lệnh tiếp theo để xuất ra thông báo Thành công.