課題２：マルウェア静的解析

配布された c2_sample.idb を静的解析し、以下の設問に答えよ。

課題２－１

当該検体の（Windows API やライブラリ関数以外の）関数呼び出しに使用されている呼出規約を以下から選べ（4 点）

- __cdecl
- __stdcall
- __fastcall
- __thiscall
- その他の呼出規約

課題２－２

関数 sub_401000 が何をする関数か答えよ（4 点）

課題２－３

暗号化の対象となるドライブの種類をすべて選択せよ（4 点）

- 固定ドライブ
- 取り外し可能ドライブ
- ネットワークドライブ
- 書き込み可能な CD/DVD ドライブ

課題２－４

関数 sub_406306 が何をする関数か答えよ（4 点）

課題２－５

当該検体が SHA-256 ハッシュ値を求めるために使用される関数 sub_404C3E は、4 番目の引数によってどのような処理の変化が起きるか答えよ（4 点）

課題２－６

当該検体のリソース EXDATA に格納されている 112 番のデータは、復号しても意味不明なデータとなるが、本来どのような情報が格納されているべきか、コードから推測せよ
(5 点)

解答

以下の URL にアクセスし、11:55 までに Google フォームから解答を提出すること。
https://goo.gl/forms/NmR9pdzxIyFBJSTi2

解答の提出には Google へのログインが必要です。
提出(Google フォームの送信)は基本的に一度で行うようにすること。
同一アカウントからの複数回の回答提出は不可です(編集は可能)