Lab # 7 - 2 — Assessment Worksheet

**Course Name and Number: IAM302**

**Student Name and Student Id:**

* **Tran Thanh Tuan – SE161095**
* **Diep Anh Vu – SE160365**
* **Shim Jun Woo – SE161064**

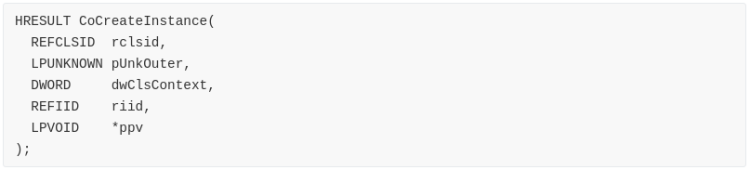
**Instructor Name: Vu Duc Ly**

## **Analyze the file Lab07-02.exe**

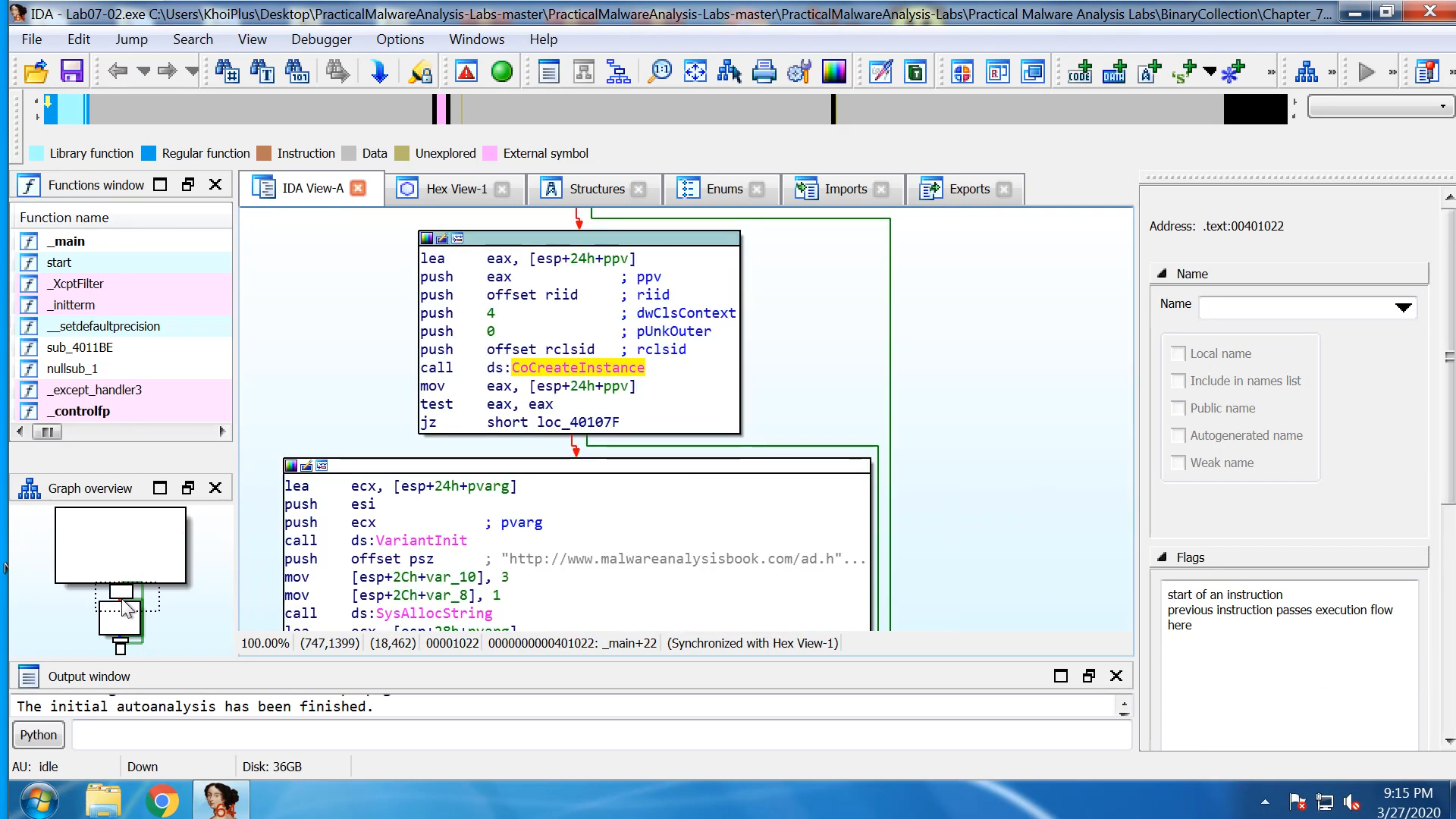
1. ***How does this program achieve persistence?***

The Malware start by using **OleInitialize**. This function is used to initialize the COM library. After that **CoCreateInstance** is used. This function creates a single uninitialized object of the class associated with a specified CLSID.

The Syntax for this function is the following:

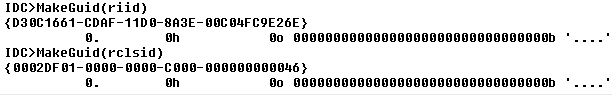


In this case, the disassembly is the following:



We need to check the **riid** and **rclsid**.

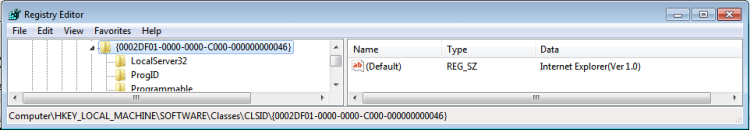
In order to get these values, I used an [IDA Plugin](https://reverseengineering.stackexchange.com/questions/17685/how-to-find-clsid-from-cocreateinstance-in-ida) that returns the identifiers of **riid** and **rclsid**. The result of the execution can be seen in the following image:



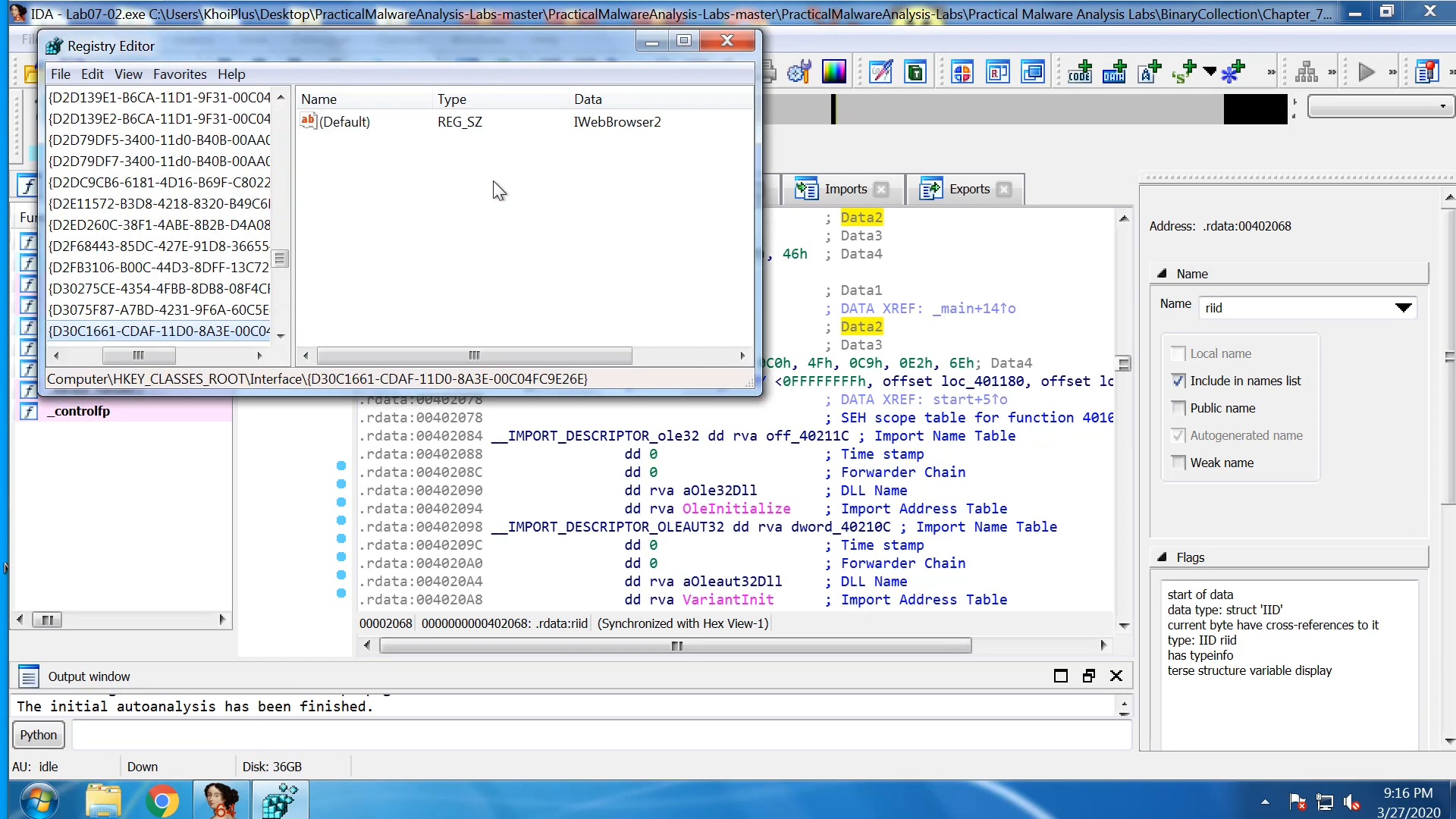
We can use Regedit in order to check the information about which code the COM Server will execute. We can use the following keys:

* HKLM\SOFTWARE\Classes\CLSID\{clsid} (to check the CLSIDs)
* HKLM\SOFTWARE\Classes\Interface\{riid} (to check the IIDs)

The **CLSID** is Internet Explorer:

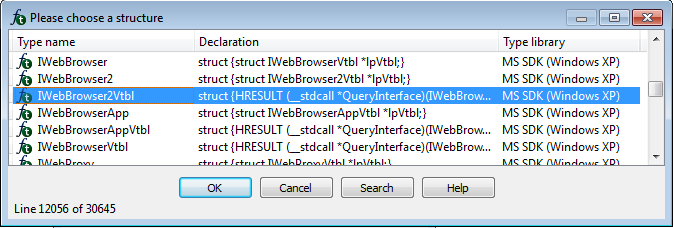


The loaded interface is **IWebBrowser2**:

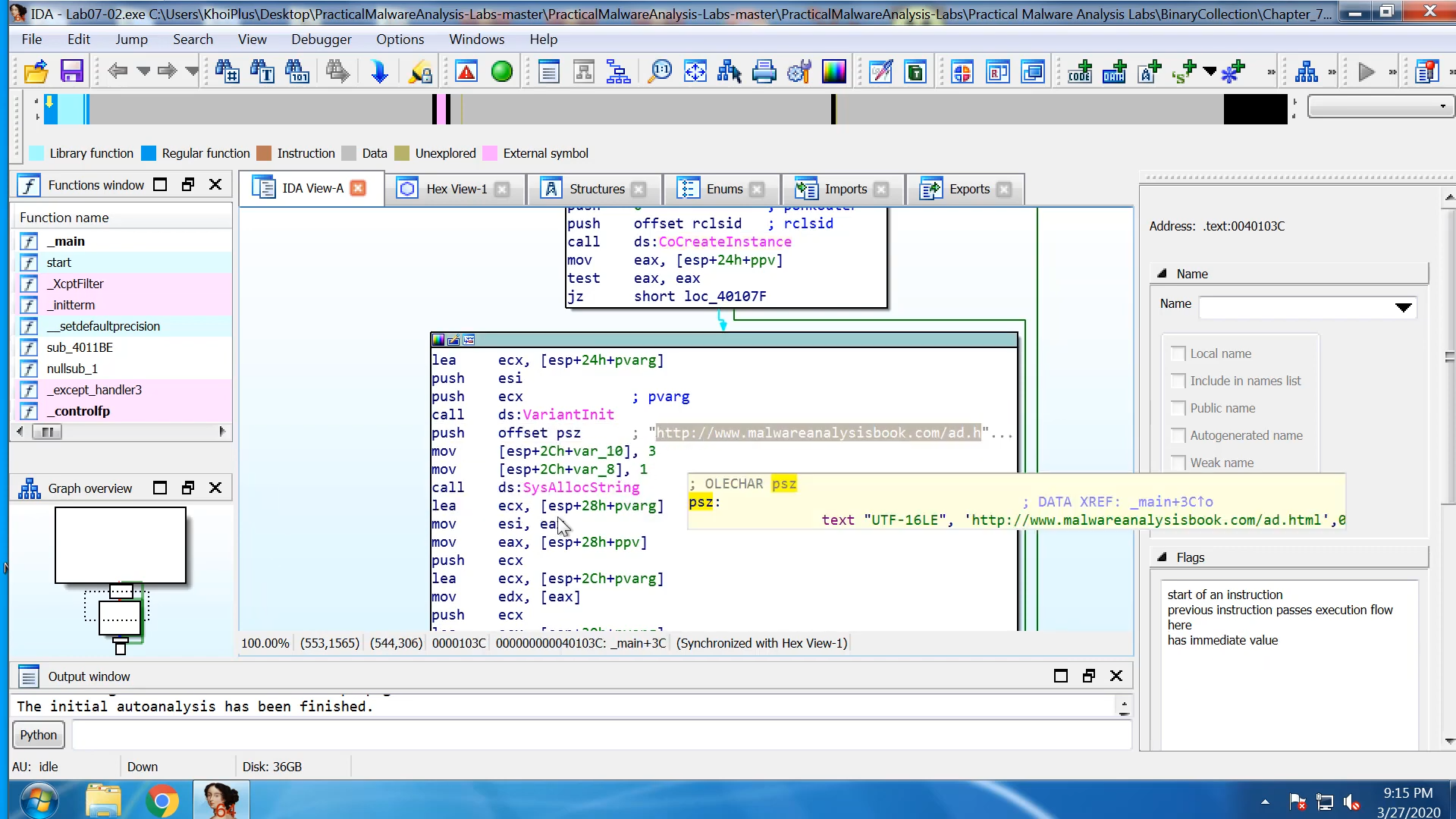


Quoting the Authors, “in order to identify what a malicious program is doing when it calls a COM function, malware analysts must determine which offset a function is stored at”.

IDA stores the offsets and Structures for common interfaces. In this case, let’s add a structure named **InterfaceNameVtbl**. For that we need to go to the Structures Tab > Press “Insert” key > Add Standard Structure and select the IWebBrowser2Vtbl structure:



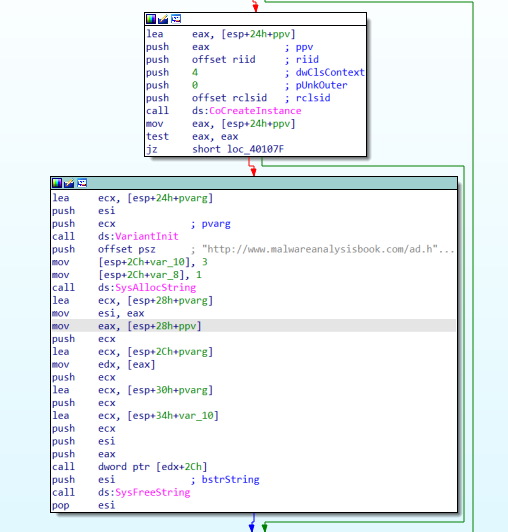
Going back to the Disassembly we can see that IDA added the comments to the call instruction:



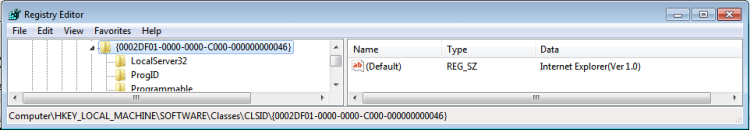
Basically, all that the Malware does is this, a simple request to <http://www.malwareanalysisbook.com/ad.html>.

Thus, the Malware doesn’t achieve persistency.

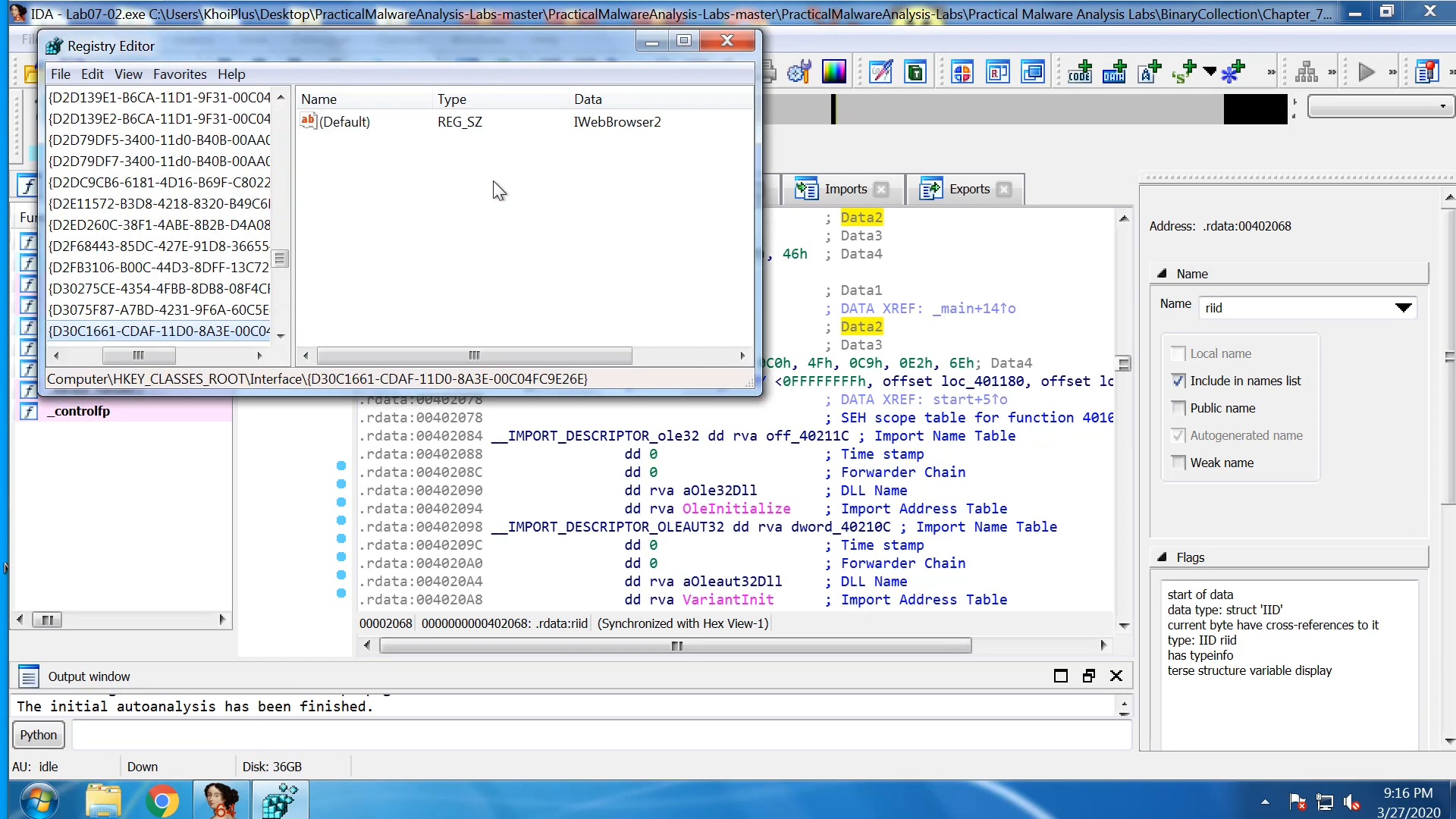
1. ***What is the purpose of this program?***

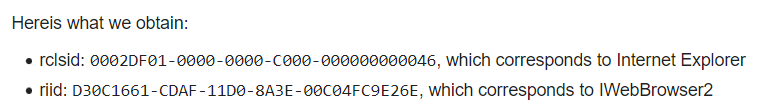


A call to CoCreateInstance was made. We can see that the rclsid is targeted to “2DF01-0000-0000-C000-000000000046”. In registry this value refers to Internet Explorer.



The riid value is set to be “D30C1661-CDAF-11D0-8A3E-00C04FC9E26” which infers to IWebBrowser2 in the registry.





Tracing down the opcodes, we will see that a call was made with offset 2Ch. It is a Navigate function call. In short on execution, a browser will pop up with the URL “[http://www.malwareanalysisbook.com/ad.html](http://www.malwareanalysisbook.com/ad.html%E2%80%9Dbeing)” being opened.

1. ***When will this program finish executing?***

Once the browser pops up and display the website, the program terminates.

