**LAB 8: IDA Pro**

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)

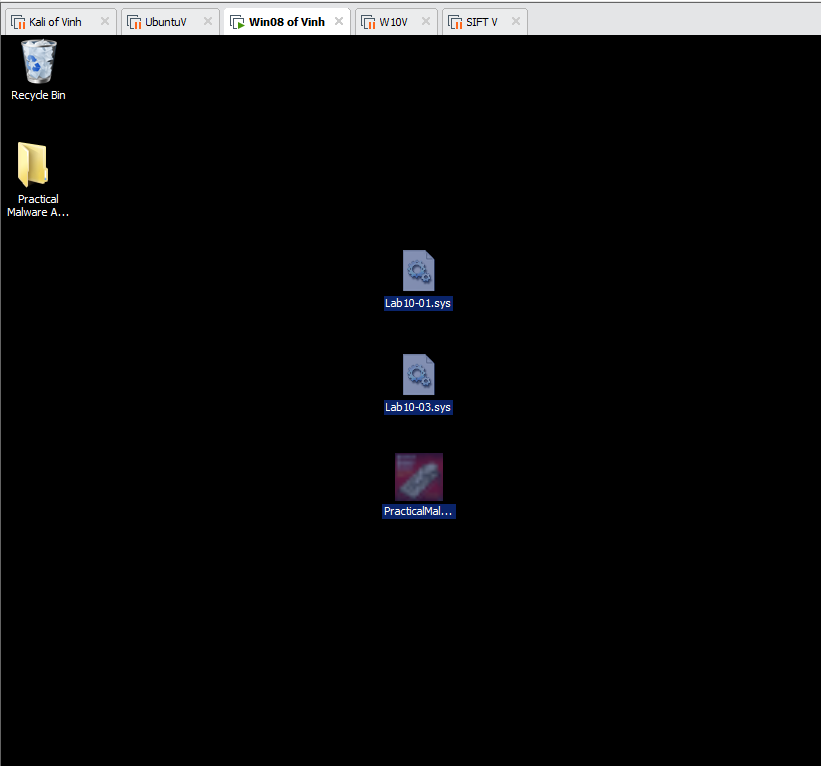
**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 15/2/2023

**Purpose**

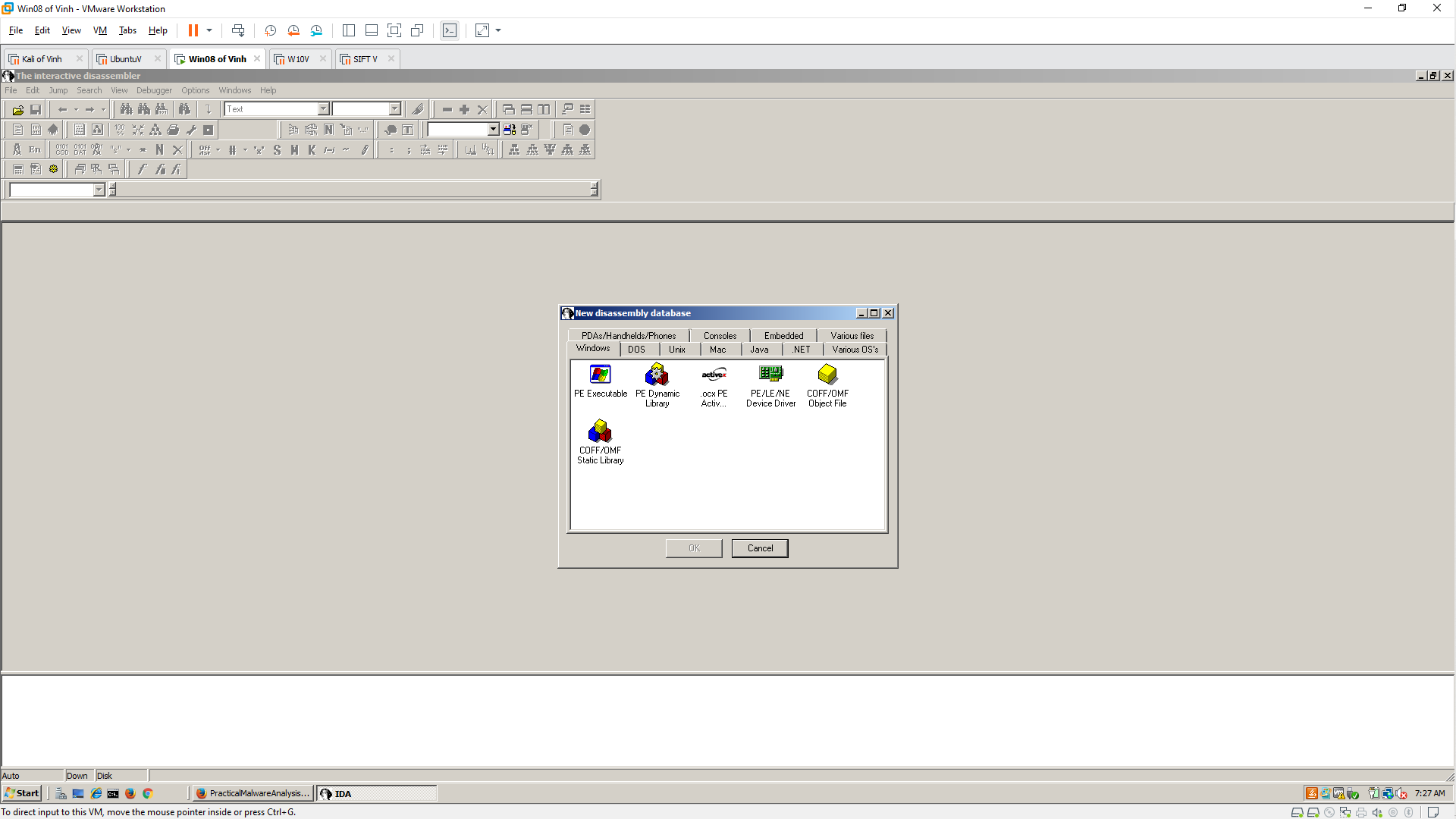
* You will practice using IDA Pro.
* You should already have the lab files



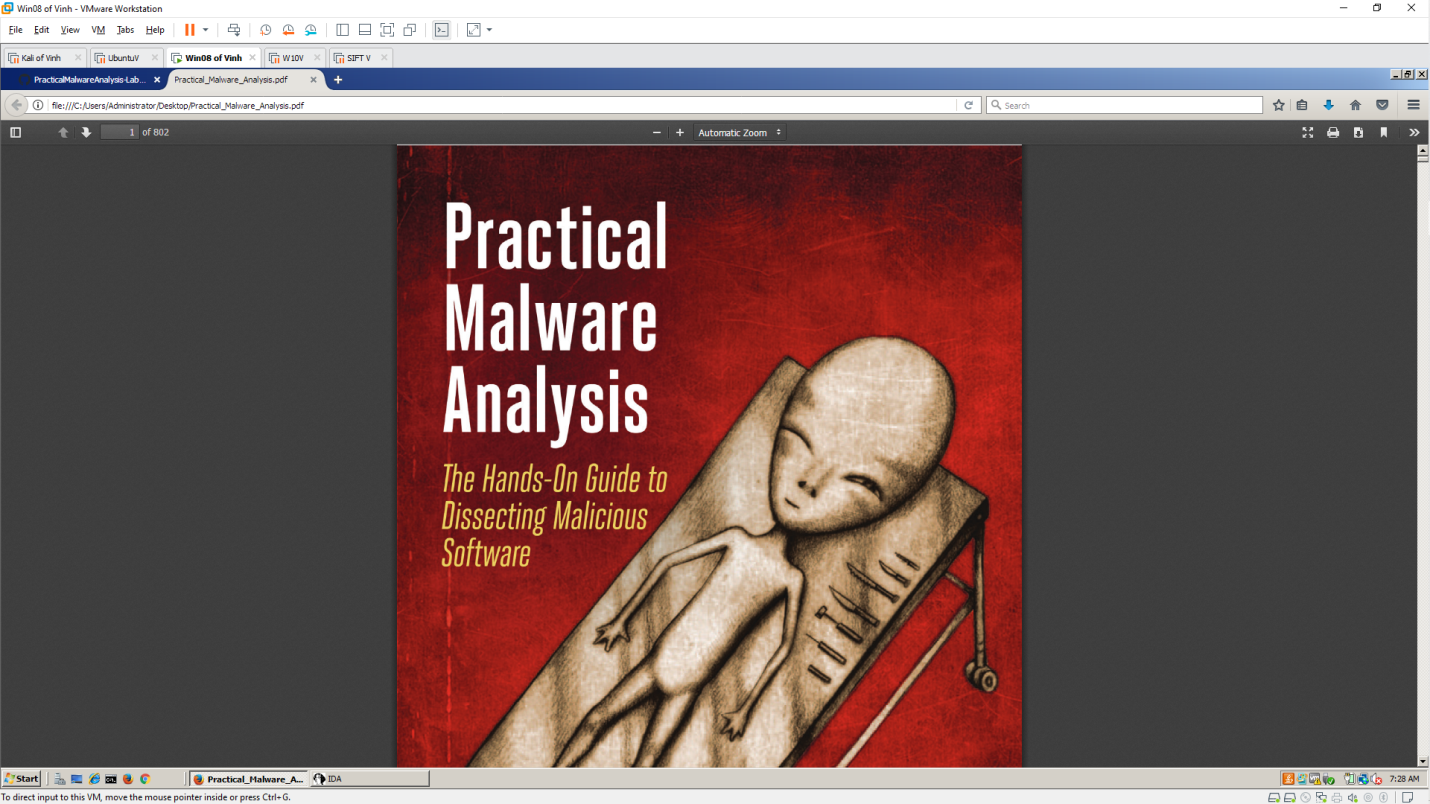
**What you need:**

* A Windows machine, real or virtual, such as the Windows 2008 Server VM we've been using
* The textbook: "Practical Malware Analysis"

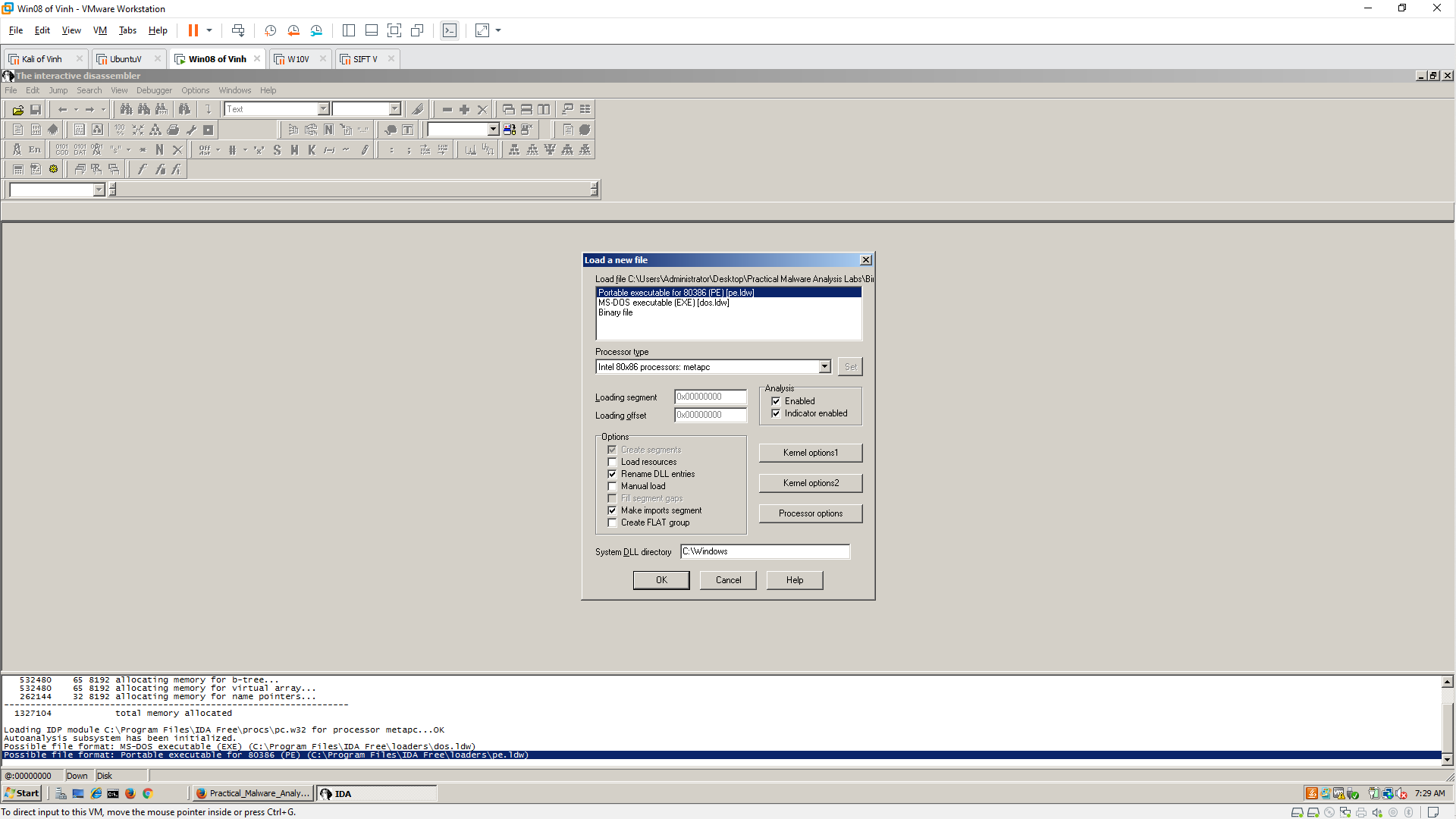
**Downloading and Installing IDA Pro**

****

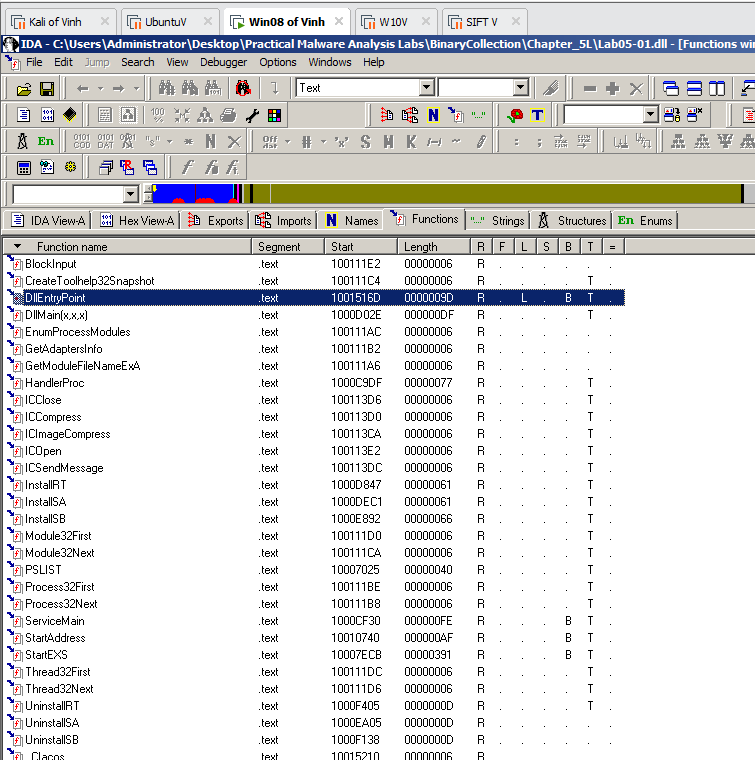
**Follow the Textbook**

****

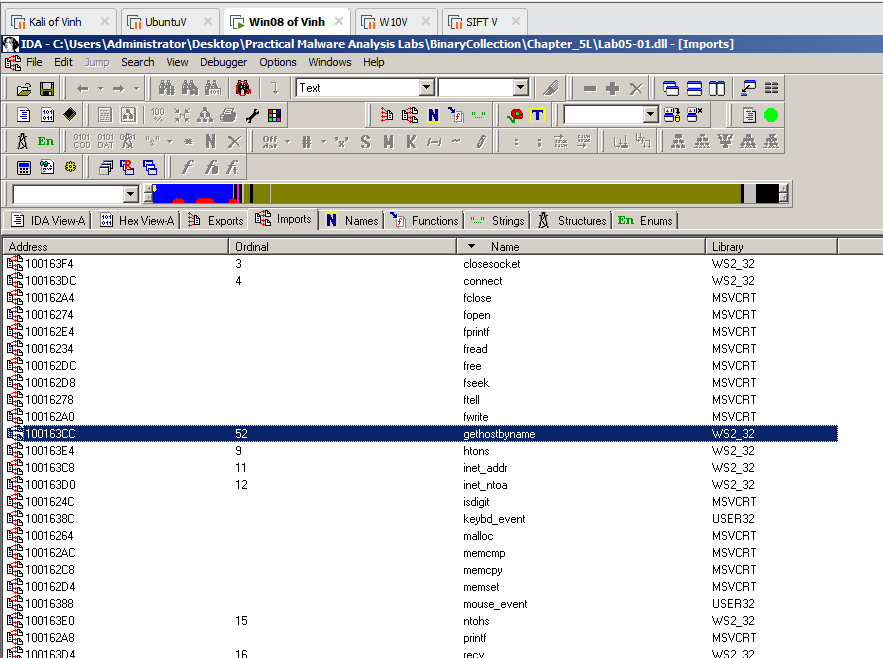
**Opening Lab05-01.dll in IDA Pro**

****

**Q1: Finding the Address of DLL Main**

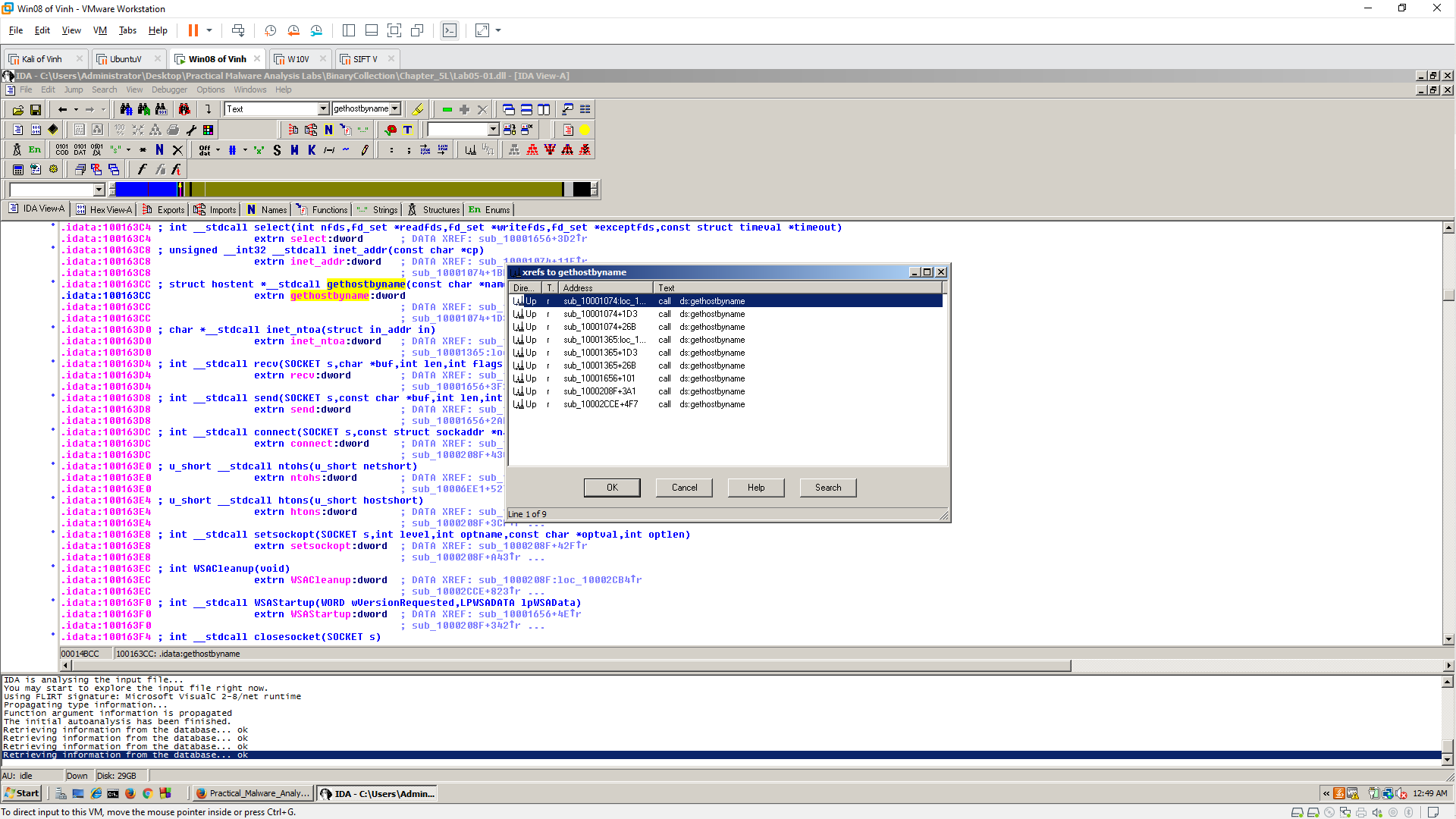
****

**Q2: Find the import for gethostbyname**

****

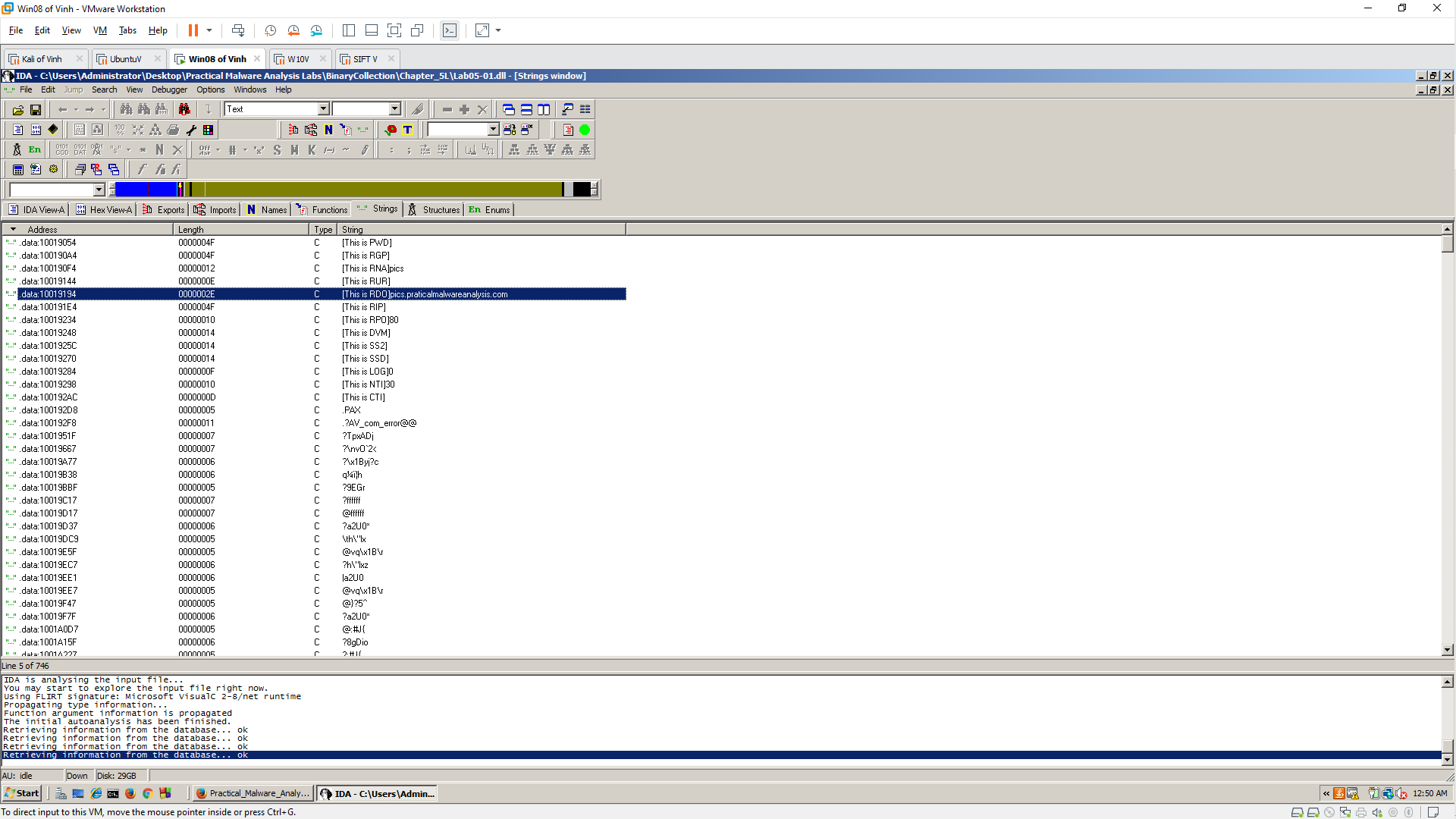
**Q3: How many functions call gethostbyname?**

* **9**

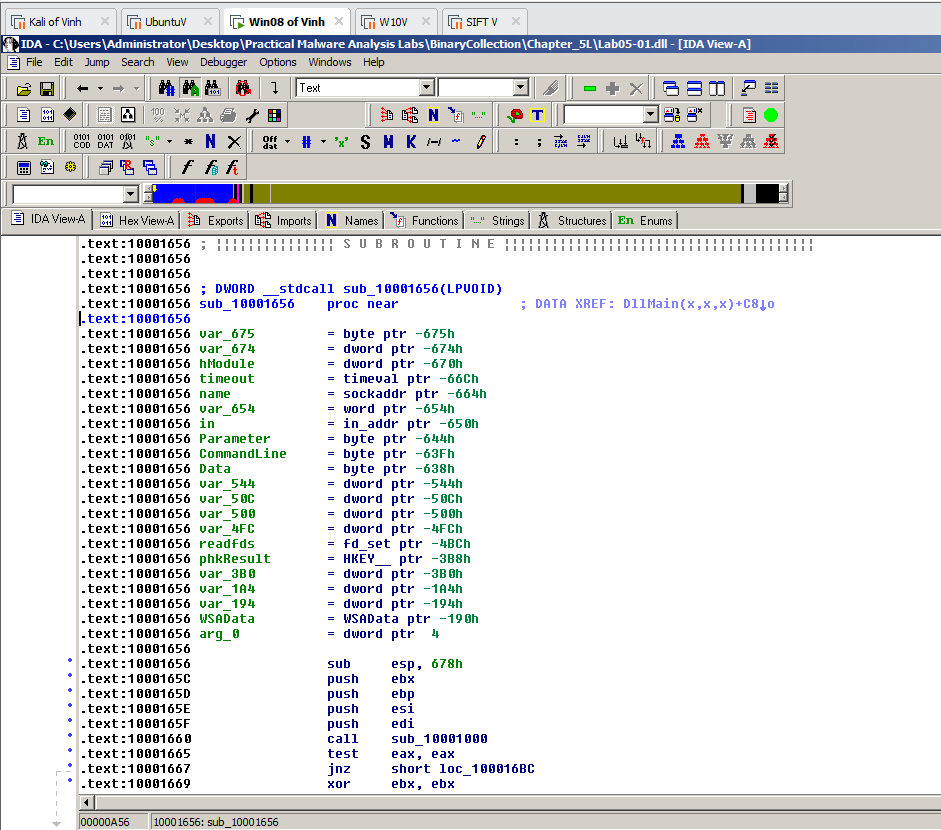
****

**Q4. Focusing on the call to gethostbyname located at 0x10001757, can you figure out which DNS request will be made?**

* **pics.praticalmalwareanalysis.com**

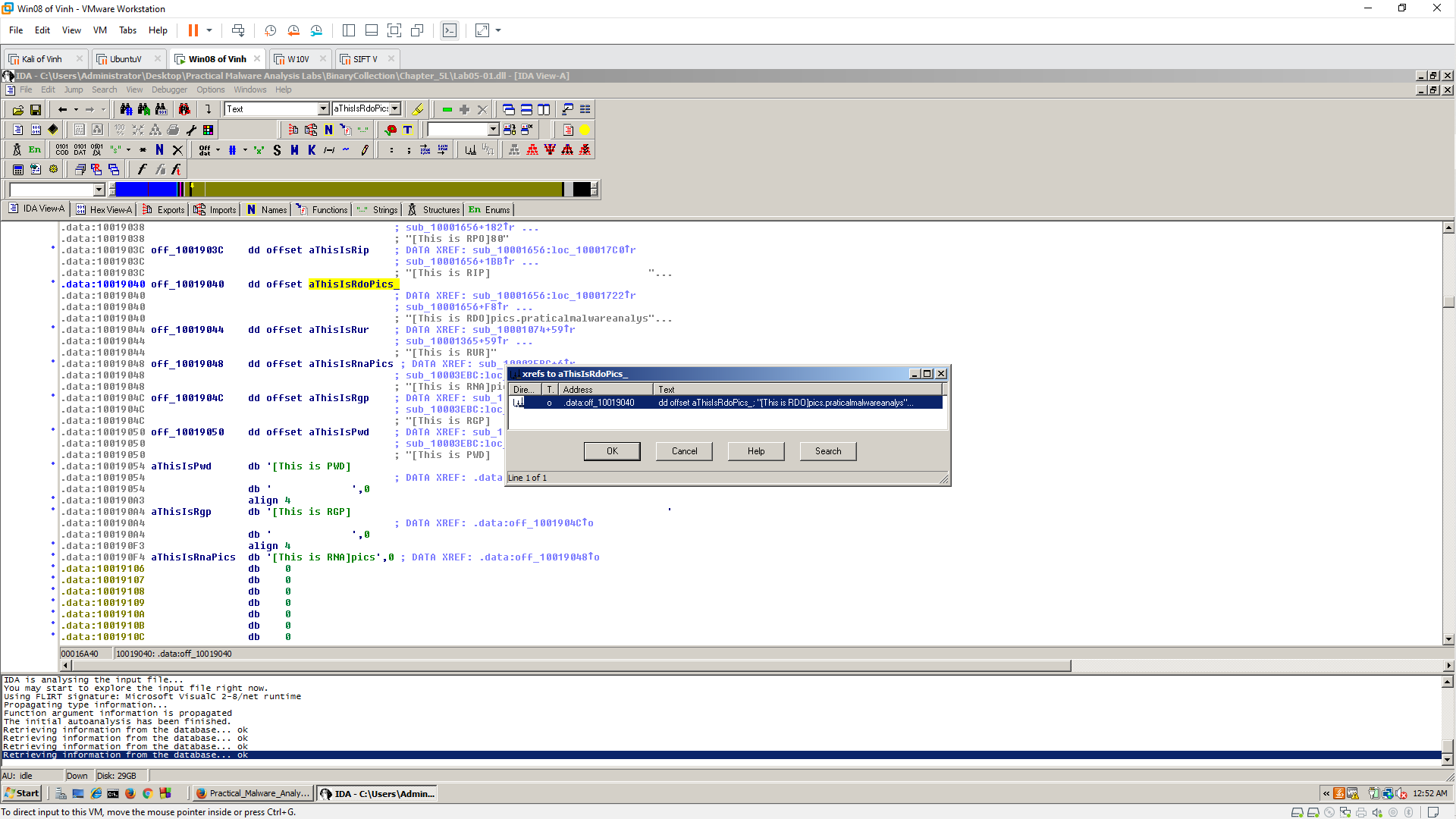
****

**Q5: Count Local Variables for the Subroutine at 0x10001656**

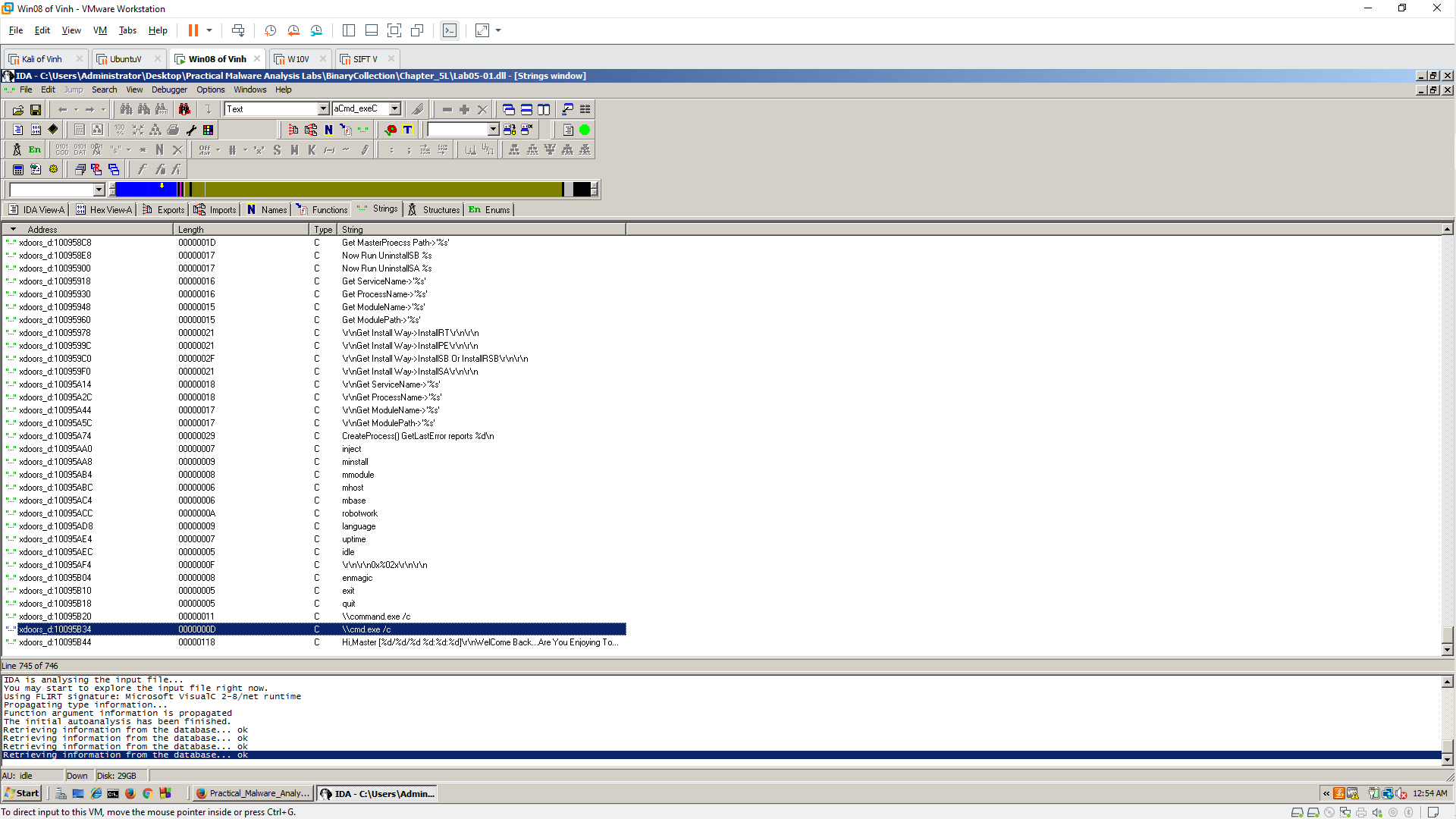
****

**Q6: How many parameters has IDA Pro recognized for the subroutine at 0x10001656?**

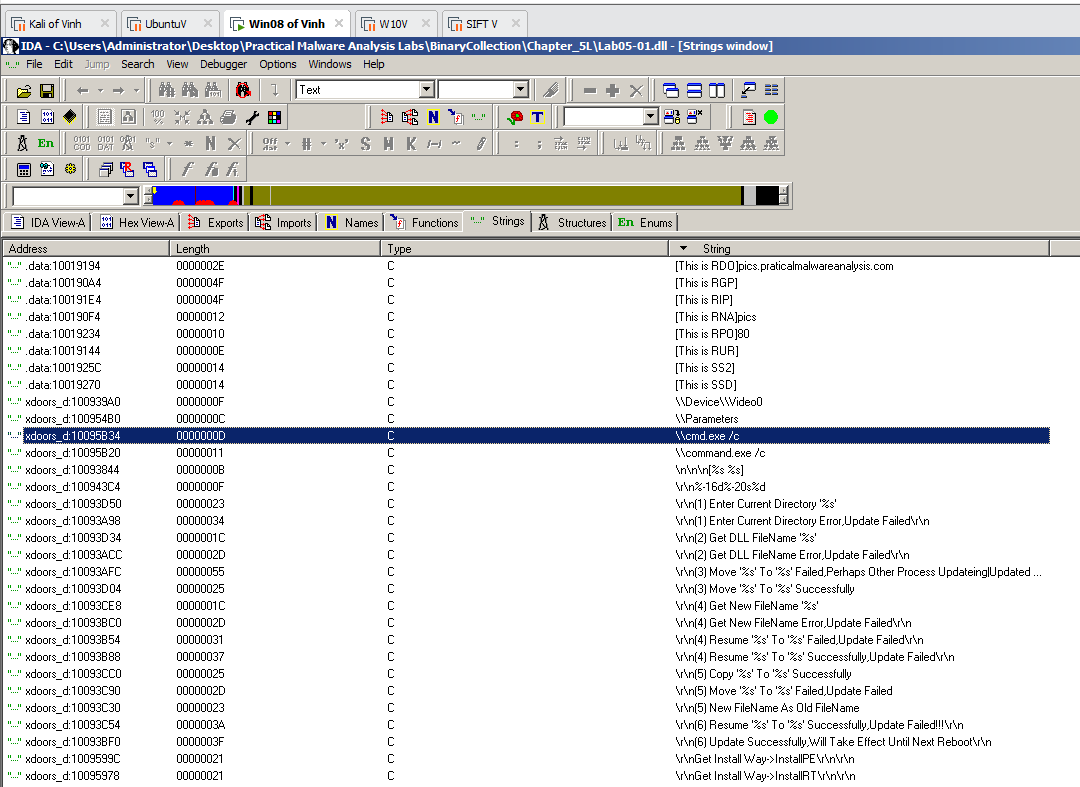
* **1**

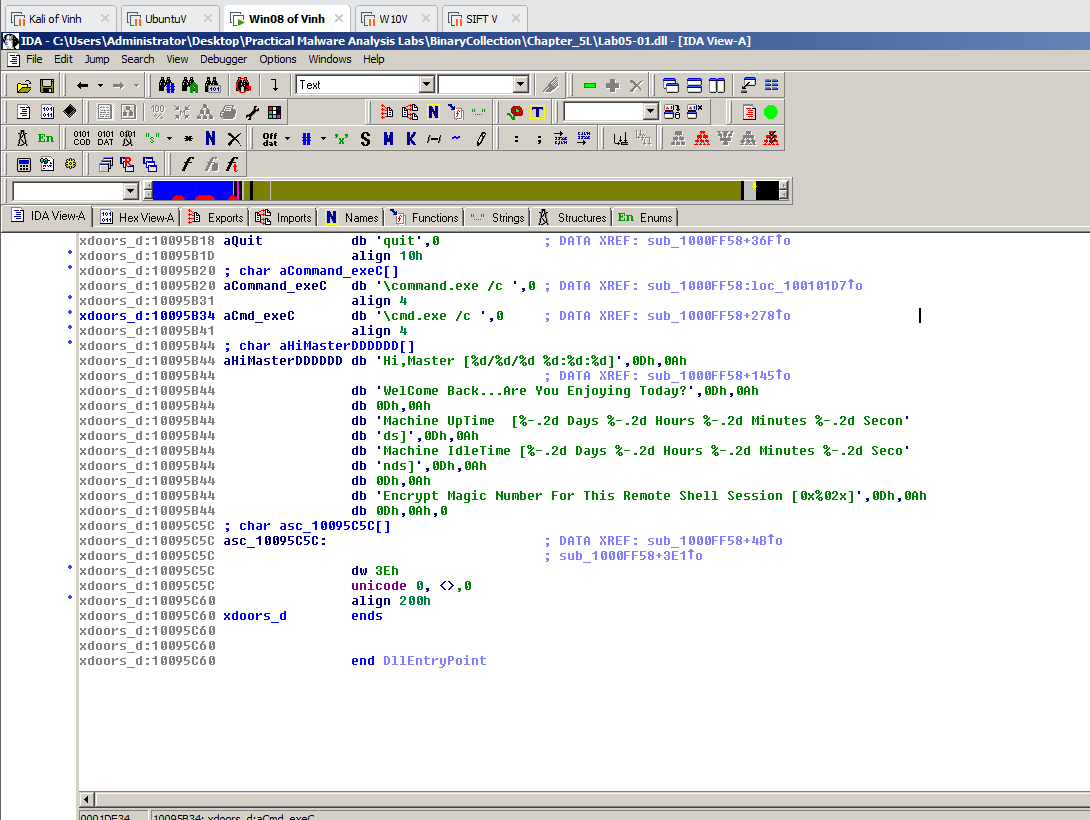
****

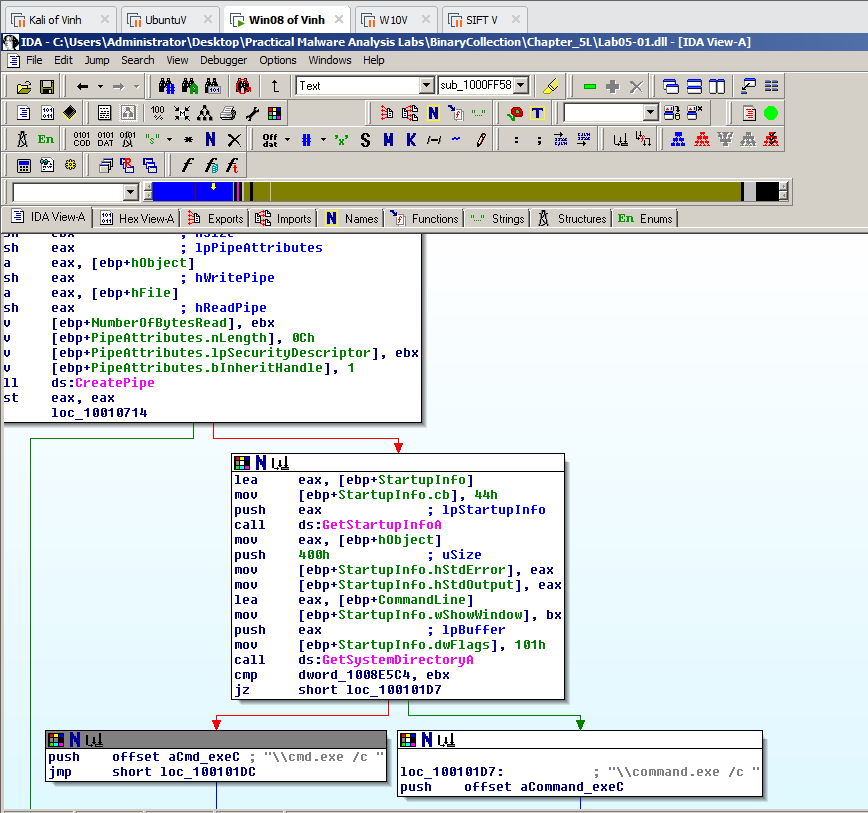
**Q7: Use the Strings window to locate the string \cmd.exe /c in the disassembly. Where is it located?**

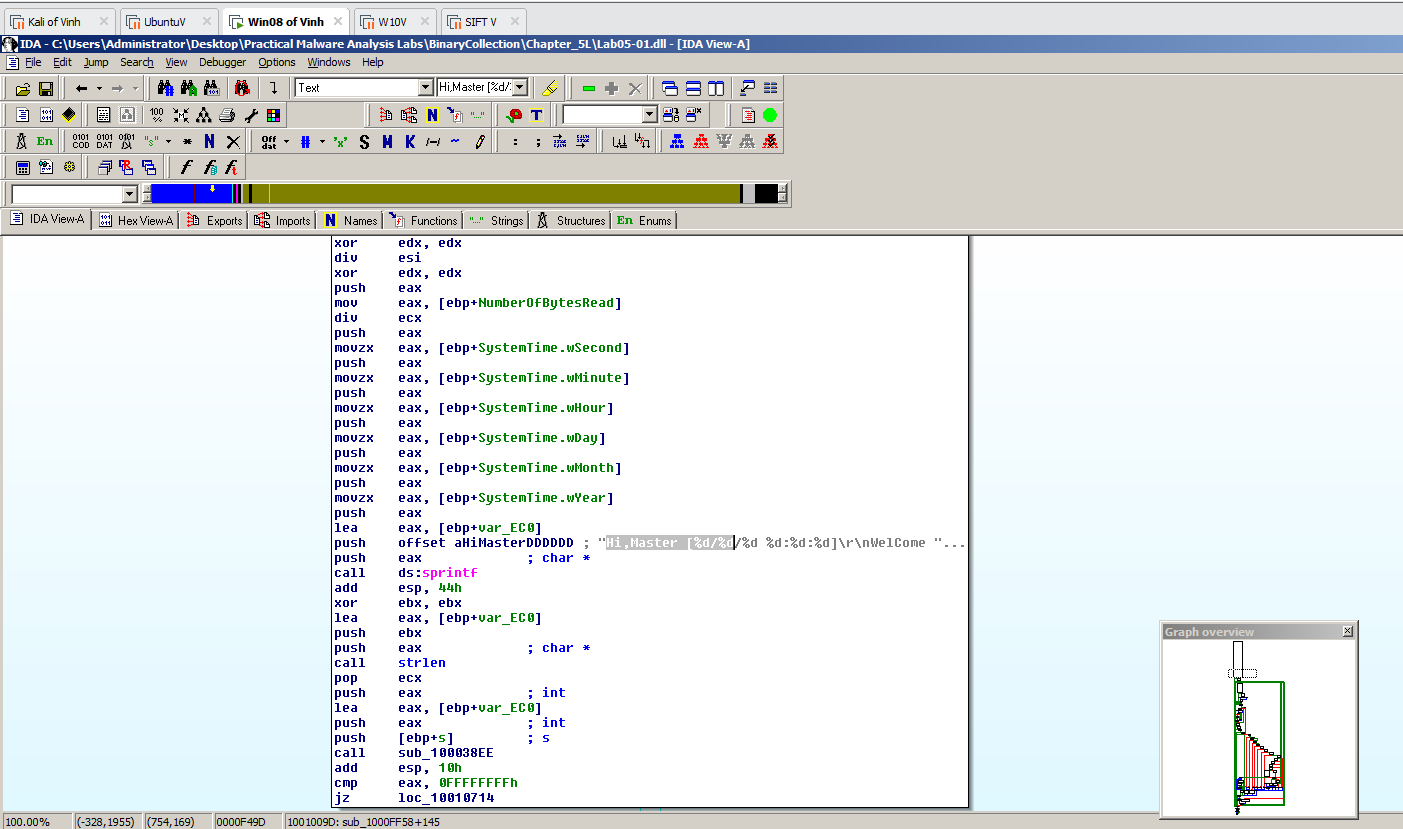
****

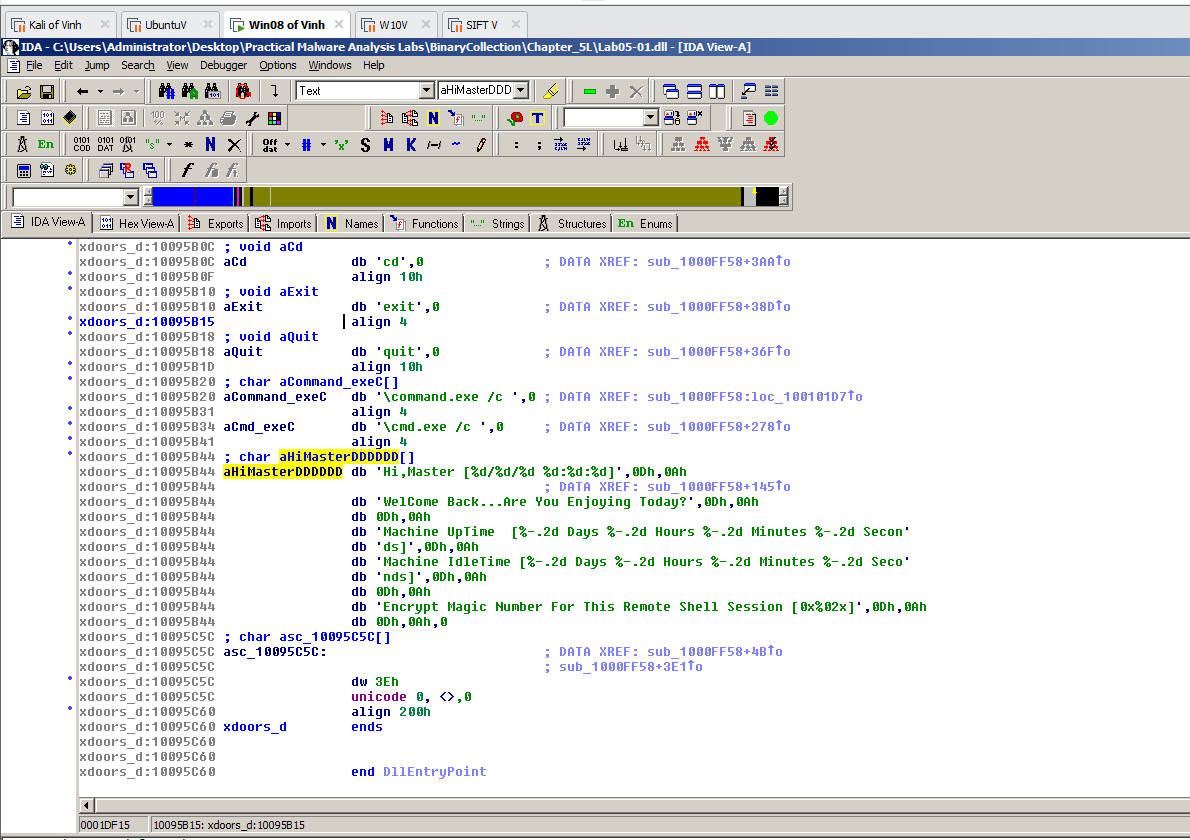
**Q8: Finding the Purpose of the Code that References \cmd.exe /c**

****

****

****

****

****