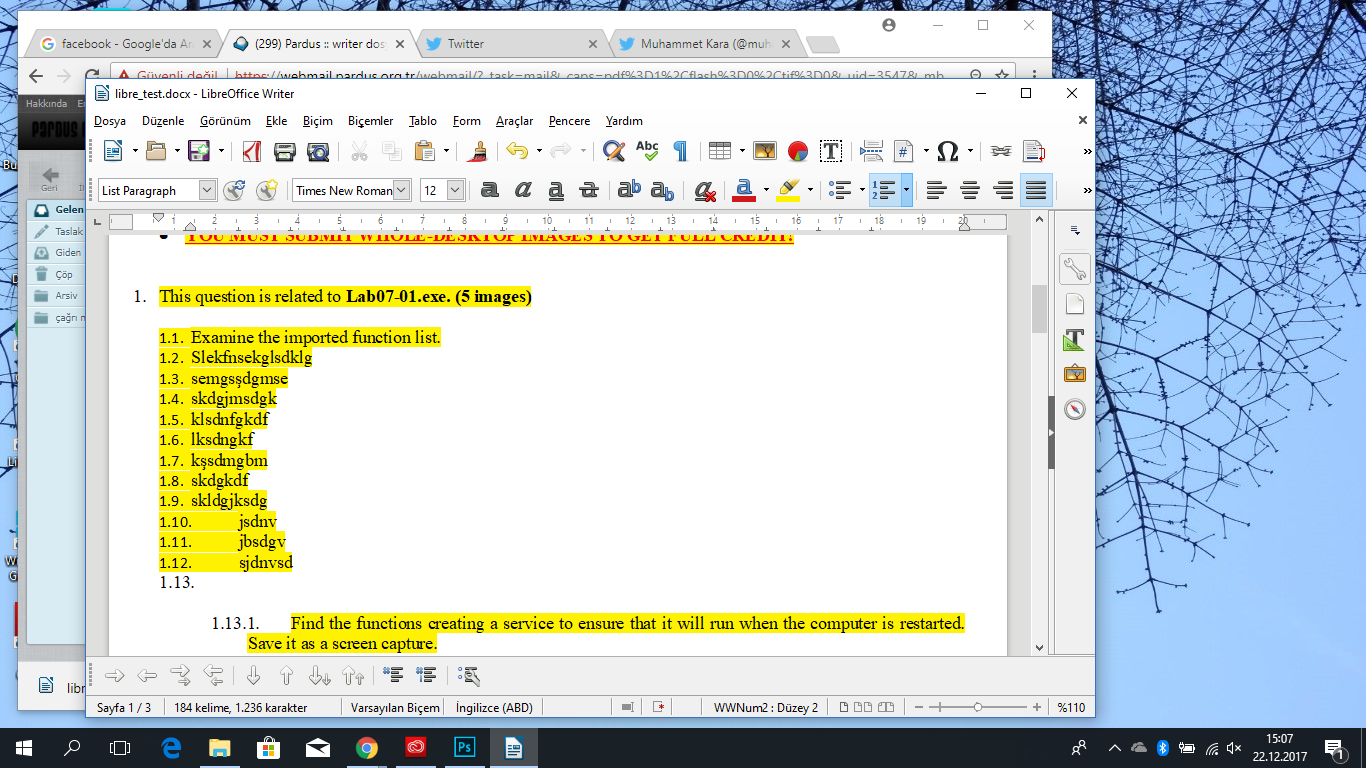
**Date:** 04/12/2017

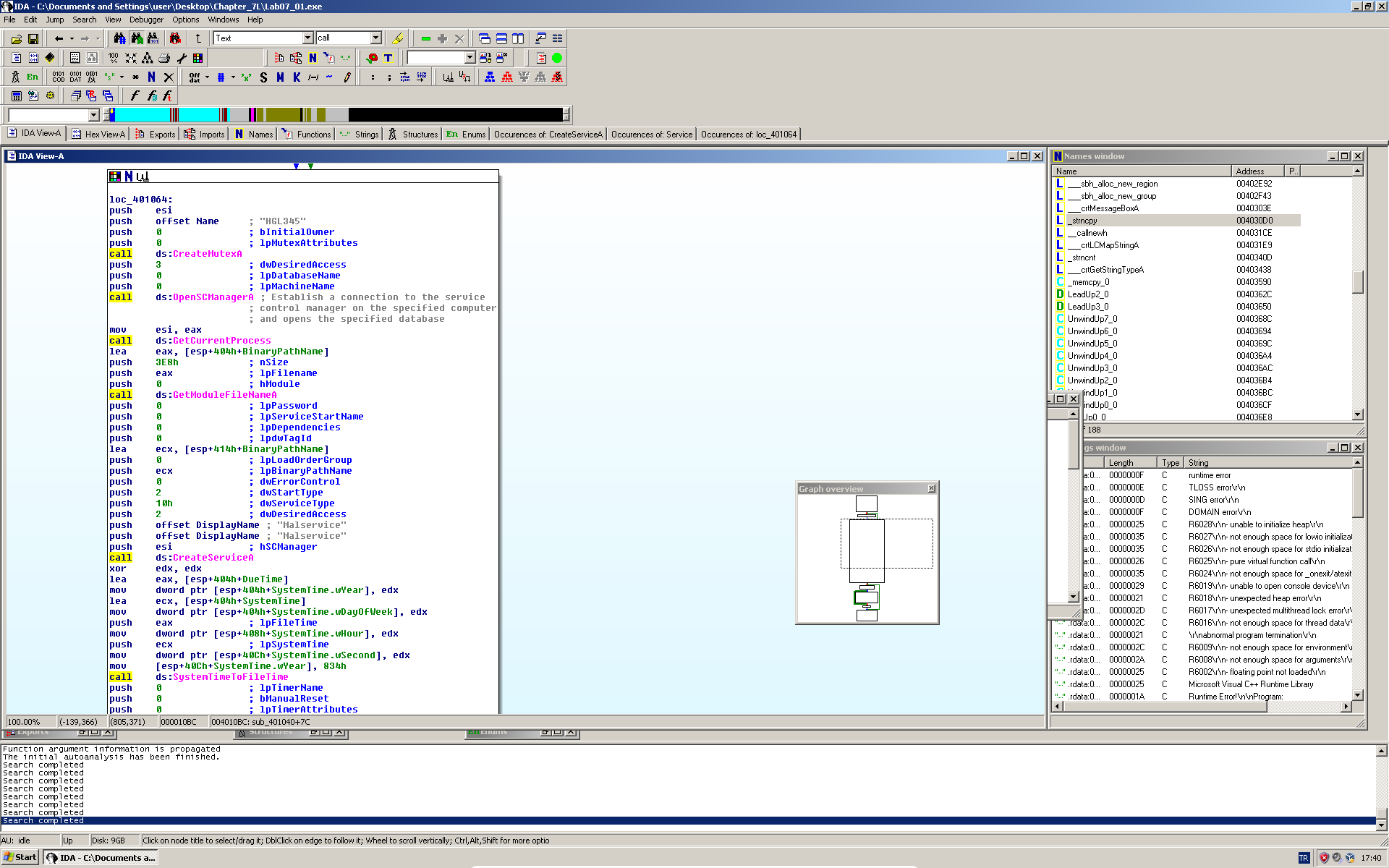
**HW8 (5 pts.)**

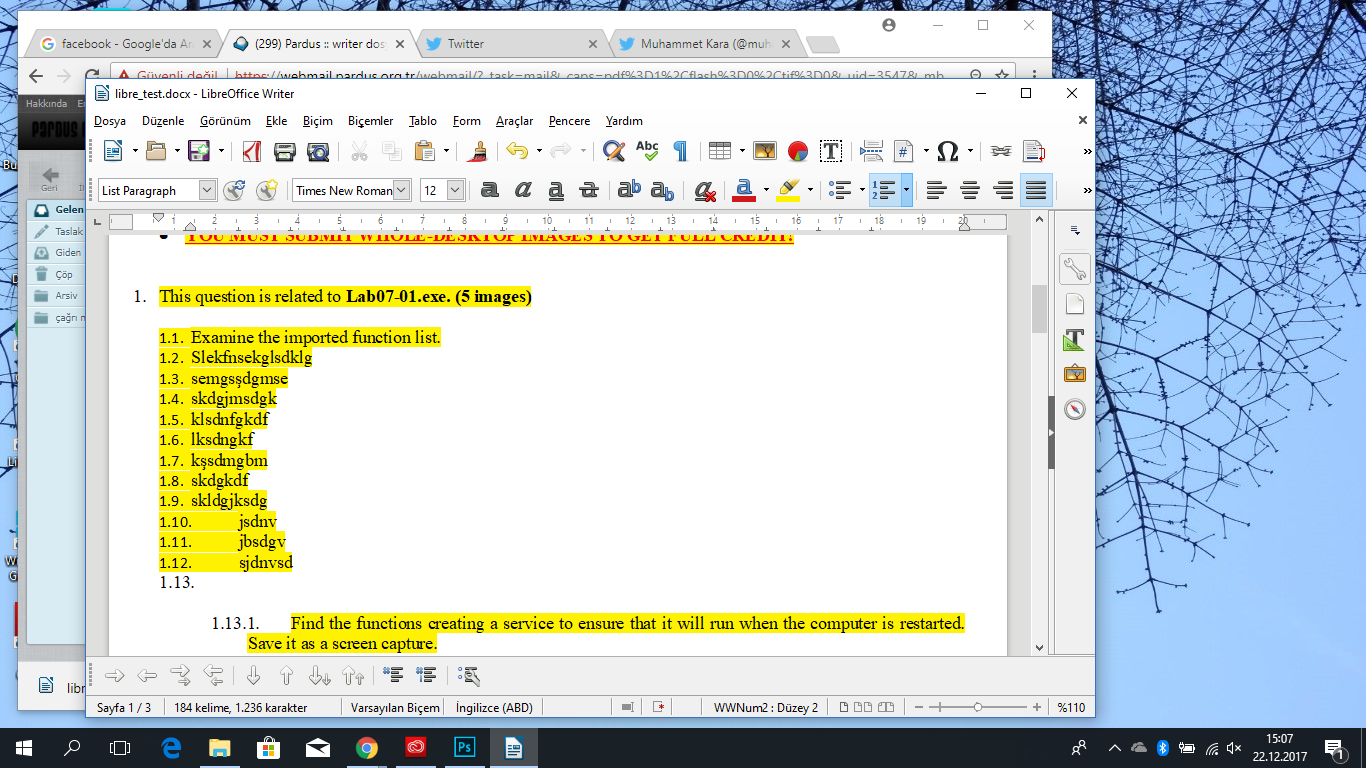
**Requirements:**

* A Windows virtual machine
* Recommended textbook: "Practical Malware Analysis"
* Get the lab files here: https://practicalmalwareanalysis.com/labs/
* This homework uses the files **Lab07-01.exe**, **Lab07-02.exe**, **Lab07-03.dll** and **Lab07-03.exe**.
* **Follow the instructions for each question, paste the images respectively IN THIS FILE, save it as "HW8.**
* **Deadline: 10/12/2017 23:59**
* **YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!**

1. This question is related to **Lab07-01.exe. (5 images)**
   1. Examine the imported function list.
   2. Slekfnsekglsdklg
   3. semgsşdgmse
   4. skdgjmsdgk
   5. klsdnfgkdf
   6. lksdngkf
   7. kşsdmgbm
   8. skdgkdf
   9. skldgjksdg
   10. jsdnv
   11. jbsdgv
   12. sjdnvsd
       1. Find the functions creating a service to ensure that it will run when the computer is restarted. Save it as a screen capture.

**\*0000000000000\*\*PASTE IMAGE HERE\*\*\***

****

* 1. Examine the imported function list.
  2. Slekfnsekglsdklg
  3. semgsşdgmse
  4. skdgjmsdgk
  5. klsdnfgkdf
  6. lksdngkf
  7. kşsdmgbm
  8. skdgkdf
  9. skldgjksdg
  10. jsdnv
  11. jbsdgv
  12. **sjdnvsd**
      1. Fill in the blanks according to the above image.
* Function 1: \_\_\_\_GetCurrentProcess\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Function 2: \_\_\_\_GetModuleFileNameA\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Function 3: \_\_\_\_CreateServiceA\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  + 1. Find the functions that might connect to a URL in order to download content. Save it as a screen capture.