Due: 3/24/2014 5:30 PM EST

CIS 484-75-4132 Project 3

Notes:

- **You will need admin access to a Windows computer for this project.**
- **All files and/or tools required for this project may be downloaded using the links posted on Blackboard or provided during lecture.**

Download the zip archive from Blackboard under Assignments\Projects\Project 3 and extract the contents of the archive. The MD5 hash of the zip file is "E35F39214631D6135661A4571C6F2908". Ensure that the MD5 hash of the zip archive you download is the same. If it's not, download the file again and recalculate the MD5 hash. Use the extracted contents of the zip archive to answer the questions below. Report all times in Eastern time.

1) Analyze the LNK files and determine:
   a) What was the full path of "2013-Sales.xlsx" when it was last opened? (2 pts)
   b) What was the full path of "Sales.xlsx" when it was last opened? (2 pts)
   c) What type of device was "Profits Graph.png" last opened from and how did you determine this information? (3 pts)
   d) What was the creation, last modified, and last accessed time of "Clients.xlsx" when it was last opened? (3 pts)
   e) Can you determine the volume serial number of the device from which "rich.pdf" was opened? If so, what is it? If not, why not? (2 pts)
   f) If the suspect that owns the machine from which these LNK files were extracted claims to have deleted "2013-Sales.xlsx" from the system on 02/20/2014, would evidence from the LNK files support or refute this claim? Explain your answer. (3 pts)
   g) If the suspect that owns the machine from which these LNK files were extracted claims to have not connected any removable storage devices to his machine after 03/01/2014, would evidence from the LNK files support or refute this claim? Explain your answer. (3 pts)
2) Analyze the jump list files and determine:
   a) When was "Personal.docx" last opened? (2 pts)
      i) What was the creation time of this file the last time it was opened? (2 pts)
      ii) What was the last modified time of this file the last time it was opened? (2 pts)
      iii) What was the full path to this file when it was last opened? (2 pts)
   b) When was "2013 list for dave.xlsx" last opened? (2 pts)
      i) What type of device was this file accessed from? (2 pts)
      ii) What is the volume name associated with the device from which this file was accessed? (2 pts)

iii) What is the volume serial number of the device from which this file was accessed? (2 pts)

c) What version of Microsoft Excel was used to open "Sales.xlsx"? How did you determine this? (2 pts)

3) Analyze the Recycle Bin and determine:
   a) When was "Personal.docx" sent to the Recycle Bin? (2 pts)
   b) When was "Clients.xlsx" sent to the Recycle Bin? (2 pts)
   c) Where was "Clients.xlsx" stored (full path) before being sent to the Recycle Bin? (2 pts)
   d) What is the size in bytes of "Tax Breaks – Acme, Inc.pdf"? (2 pts)
   e) What is the name of the file that you would expect to hold the file content of "2013-Sales.xlsx" in the Recycle Bin? How do you know this? (2 pts)
   f) Can you determine how many different user accounts have files in the Recycle Bin? If so, how many and how did you determine your answer? (2 pts)
4) Analyze the registry hives and determine:
   a) What operating system and service pack is installed on the system? (2 pts)
   b) When was the operating system installed? (2 pts)
   c) How many USB storage devices have been connected to the system? (2 pts)
      i) What is the serial number of each USB device? (2 pts)
   d) How many user accounts are on the system? (2 pts)
      i) What is the name of each user account? (3 pts)
   e) Are any of the user accounts password protected? If so, which one(s)? (3 pts)
   f) What websites have been typed into the Internet Explorer address bar? (2 pts)
      i) When was the last URL entered into the address bar? How did you determine this? (4 pts)
   g) What is the computer name of the system? (2 pts)
      i) Does it appear that the computer name been changed since the operating system was installed? If so, when? How did you determine this? (4 pts)
   h) How many times has the "Win7" user logged in? (2 pts)
5) Using any combination of the LNK files, jump lists, Recycle Bin, and provided registry hives, determine the following:
   a) What is the user name of the account that sent "Manna.doc" to the Recycle Bin? How did you determine this? (6 pts)
   b) What was the original computer name of the system? How did you determine this? (6 pts)
6) Record any and all equipment that you used for this project (hardware and software). This should include operating system version, type of flash drive, etc. (5 pts)
7) Use complete sentences and proper grammar throughout your write-up. Denote specifically which section/question you are answering in your write-up (e.g. 1-A, 1-B, etc.). (5 pts)