**CIS 484-75-4182 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.**
* **Submit your answers via the BlackBoard assessment under Projects & Labs\Project 3.**

*Download the Project3.E01 file from Blackboard under Projects & Labs\Project 3 and verify the integrity of the image after downloading (open image in FTK Imager*  *right-click on image -* *verify Drive/Image). If the image verification is unsuccessful, try downloading the re-verifying the image file. Extract the contents of the image file and answer the questions below.* ***Report all times in UTC****.*

**Analyze the LNK files and jump lists and determine:**

1. What was the full path of “2013-Sales.xlsx” when it was last opened? (2 pts)

C:\Users\Win7\Documents\2013-Sales.xlsx

1. What type of device was “Profits Graph.png” accessed from? (2 pts)

Removable storage media E:

1. When was “2013 list for dave.xlsx” last opened? (2 pts)

3/2/2014 5:00

1. What type of device was “2013 list for dave.xlsx” accessed from? (2 pts)

Removable Storage Media

1. What was the last modified time of “Clients.xlsx” when it was last opened? (2 pts)

2014-03-02 18:50:12

1. What is the volume serial number of the device from which “rich.pdf” was opened? (2 pts)

B4A2B40D

1. What version of Microsoft Excel was used to open “Sales.xlsx”? (2 pts)

2007

1. What was the full path to “Personal.docx” when it was last opened? (2 pts)

C:\Users\Win7\Documents\Personal.docx

1. If the suspect that owns the machine from which these LNK files and jump lists 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)

Evidence would refute this claim because the 2013-Sales.xlsx file was accessed on 3/2/2014 18:45. Many days after the suspect claimed the file was deleted.

1. If the suspect that owns the machine from which these LNK files and jump lists 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)

Evidence would refute this claim because the Clients.lnk file was last modified on 2014-03-02 18:50:12 from a removable storage media.

1. Explain how LNK files and jump lists can be helpful in a forensic investigation. (3 pts)

They are helpful in a forensic investigation because they both show when a suspect has accessed certain files. Also, lnk files provide data on file paths of specific files, drive serial numbers providing where files were stored. Jump lists basically provide the same information but are stored in a different way.

**Analyze the Recycle Bin and determine:**

1. When was “Personal.docx” sent to the Recycle Bin? (2 pts)
2. When was “Clients.xlsx” sent to the Recycle Bin? (2 pts)
3. Where was “Clients.xlsx” stored (full path) before being sent to the Recycle Bin? (2 pts)
4. What is the size in bytes of “Tax Breaks – Acme, Inc.pdf”? (2 pts)
5. What is the name of the file that you would expect to hold the file content of “2013Sales.xlsx” in the Recycle Bin? (2 pts)
6. How many different user accounts have files in the Recycle Bin? (2 pts)
7. Explain how recycle bin analysis can be helpful in a forensic investigation. (3 pts)

**Analyze the registry hives and determine:**

1. What operating system and service pack is installed on the system? (2 pts)

Windows 7 professional service pack 1

1. When was the operating system installed? (2 pts)

Sat, 04 Aug 2012 13:21:00

1. What programs are configured to start each time the system boots? (2 pts)

VMware User Process, VMware tools, MSC

1. How many USB storage devices have been connected to the system and what is the serial number of each USB device? (4 pts)
2. What is the name of each user account on the system? (3 pts)
3. Which user accounts password protected? (2 pts)
4. What is the name of the program executed on 1/5/2013 from a user’s desktop? (2 pts)
5. What websites have been typed into the Internet Explorer address bar? (2 pts)
6. What day and time was the last URL entered into the address bar? (3 pts)
7. What is the computer name of the system? (2 pts)
8. Does it appear that the computer name been changed since the operating system was installed? If so, when? How did you determine this? (3 pts)
9. How many times has the “Win7” user logged in? (2 pts)
10. Explain how registry analysis can be helpful in a forensic investigation. (3 pts)

**Analyze the scheduled tasks and determine:**

1. How often is GoogleUpdate.exe scheduled to execute? (2 pts)
2. When is the “dkfo4f” scheduled task configured to execute? (2 pts)
3. When was the “dkfo4f” create and what account was it created by? (2 pts)
4. Do any of the scheduled tasks seem suspicious? If so, which ones and why? (2 pts)

**Using any combination of the LNK files, jump lists, Recycle Bin, scheduled tasks, and provided** **registry hives, determine the following:**

1. What is the user name of the account that sent “Manna.doc” to the Recycle Bin? How did you determine this? (5 pts)
2. What was the original computer name of the system? How did you determine this? (5 pts)
3. What is the manufacturer, model, and serial number (not volume serial number) of the device from which “rich.pdf” was opened? How did you determine this? (5 pts)

1. 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)