**CIS 484-77-4188 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\Project 3.**

*Download the Project3.E01 file from Blackboard under Projects\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**
2. What type of device was “Profits Graph.png” accessed from? (2 pts) **E: is listed in the path or a removable storage media (Floppy, USB)**
3. When was “2013 list for dave.xlsx” last opened? (2 pts) **03/02/2014 at 18:45**
4. What type of device was “2013 list for dave.xlsx” accessed from? (2 pts) **2013 List for Dave.xlsx is accessed from E: removable disk (Floppy or USB)**
5. What was the last modified time of “Clients.xlsx” when it was last opened? (2 pts) **The last modified time for Clients.xlsx is 03-02-2014 at 18:50.**
6. What is the volume serial number of the device from which “rich.pdf” was opened? (2 pts) **B4A2B40D**
7. What version of Microsoft Excel was used to open “Sales.xlsx”? (2 pts) **Microsoft Excel 2007 was used to open Sales.xlsx**
8. What was the full path to “Personal.docx” when it was last opened? (2 pts) **C:\Users\Win7\Documents\Personal.docx**
9. 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)

**The evidence would prove this claim wrong because the suspect’s last accessed time is 03/02/2014 18:45 on the target accessed so the file could not have been deleted on 02/20/2014.**

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)

**The evidence would prove this claim wrong because rich.pdf, Profits Graphh.png and clients.xslx were accessed through the removable device on 03/02/2014.**

1. Explain how LNK files and jump lists can be helpful in a forensic investigation. (3 pts) **Analyze the Recycle Bin and determine:**

**LNK files and jump lists can show when a suspect accessed some files. LNK files provides metadata on files which includes when the file was created, last accessed, modified, file paths of files and drive serial numbers of where the files are stored. Jump lists provide the same information but they are stored in a different way. They use one jump list per application.**

1. When was “Personal.docx” sent to the Recycle Bin? (2 pts) **3/2/2014 18:51**
2. When was “Clients.xlsx” sent to the Recycle Bin? (2 pts) **3/2/2014 18:51**
3. Where was “Clients.xlsx” stored (full path) before being sent to the Recycle Bin? (2 pts)

**C:\Users\Win7\Documents\Clients.xlsx**

1. What is the size in bytes of “Tax Breaks – Acme, Inc.pdf”? (2 pts)

**402107 bytes**

1. 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)

**‘$IWN9JUT.xlsx’**

1. How many different user accounts have files in the Recycle Bin? (2 pts)

**2 users : Josh and Win7**

1. Explain how recycle bin analysis can be helpful in a forensic investigation. (3 pts)

**The Recycle bin analysis can be useful in a forensic investigation because, you can see dates and times deleted, file name, file paths, file size, and OS versions of files that may be relevant in a forensics case. This information can be used in court to argue a case.**

**Analyze the registry hives and determine:**

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

**Windows 7 Professional and Service pack 1**

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

**07/14/2009 04:53:25**

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

**VMWare, VMWare User Process, 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)

**There have been two USB drives connected to the machine. Their serial numbers are: 0013729B678DEB20C51F0216&0 and 4859701DEF10326C&0.**

1. What is the name of each user account on the system? (3 pts)

**Administrator, Guest, Win7 and Josh.**

1. Which user accounts password protected? (2 pts)

**Administrator, Guest, Win7 and Josh requires passwords**

1. What is the name of the program executed on 1/5/2013 from a user’s desktop? (2 pts)

**The name of the program is X12-30307.exe**

1. What websites have been typed into the Internet Explorer address bar? (2 pts)

**The URls that have been typed searched in Microsoft Explorer’s address bar:**

**http://skydrive.com/,**

[**http://dropbox.com/**](http://dropbox.com/)**,**

[**http://outlook.com/**](http://outlook.com/)**,**

**http: //louisville.edu/,**

[**https://www.google.com/**](https://www.google.com/)**,**

[**http://www.amazon.com/**](http://www.amazon.com/)**,**

**http:/ /www.overstock.com/,**

[**http://go.microsoft.com/fwlink/?LinkId=69157**](http://go.microsoft.com/fwlink/?LinkId=69157)

1. What day and time was the last URL entered into the address bar? (3 pts)

**Sunday 03/02/2014 19:25:17**

1. What is the computer name of the system? (2 pts)

**ComputerName = ACME-WORKSTATION**

1. 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)

**It seems like the computer name has been changed since the operating system was installed, it has been changed from mnmsrvc to ACME-WORKSTATION. Time is 03-02-2014 19:26:43. I determined this by looking at the Last Write Date on Expansion and because there were two entries and one said default.**

1. How many times has the “Win7” user logged in? (2 pts)

**11 times**

1. Explain how registry analysis can be helpful in a forensic investigation. (3 pts)

**Registry analysis can be helpful in a forensic investigation because the registry can record many actions that a user takes on a system, it provides vast amount of information about the computer, the operating system, the applications on the system, and user activity, typed URL’s, password information, etc. It allows them to see what devices have been connected to the machine, as well as the programs that run when the computer is booted.**

**Analyze the scheduled tasks and determine:**

1. How often is GoogleUpdate.exe scheduled to execute? (2 pts)

**Once every day**

1. When is the “dkfo4f” scheduled task configured to execute? (2 pts)

**When the Win7 user logs in**

1. When was the “dkfo4f” create and what account was it created by? (2 pts)

**This was created on 06/20/2013 at 11:28:50 by a Guest account.**

1. Do any of the scheduled tasks seem suspicious? If so, which ones and why? (2 pts)

**Yes, there are some tasks that seem suspicious. “dkfo4f” is created by the Guest account and it seems suspicious because it runs every time a user logs in.**

**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)

**The user name Josh sent “Manna.doc” to the recycle bin and I determined this by going to the FTK Imager under SID showing in the recycle bin. I just searched for it in the software registry and was able to find the account that is associated with the SID.**

1. What was the original computer name of the system? How did you determine this? (5 pts)

**The Original Computer Name is WIN-LPUE2OJ805Q. I determined this when I was looking at the dkfo4f task which showed a different computer name than ACME-WORKSTATION.**

1. 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)

**Manufacturer – SanDisk**

**Model – Cruzer Micro**

**Serial Number - 4859701DEF10326C&0**

**I determined this by looking at the LNK file and then I converted the hex volume serial number (B4A2B40D) to decimal and matched up in EMDManagement.**

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)

**Laptop Model - ASUS – Q534UXK**

**Windows 10**

**FTK Imager**

**Registry Explorer**

**Notepad**

**XML Notepad**

**LECmd**

**JLECmd**

**Command Prompt**

**$IParse**

**MFT Stampede**

**RegRipper**