Fenn Due: 03/16/2020 5:30 PM

CIS 484-75-4202 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

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

Removable storage media (Floppy, USB)

3) When was "2013 list for dave.xlsx" last opened? (2 pts)

3/2/2014 19:30

4) What type of device was "2013 list for dave.xlsx" accessed from? (2 pts)

Removable storage media (Floppy, USB)

5) What was the last modified time of "Clients.xlsx" when it was last opened? (2 pts)

3/2/2014 18:45

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 Office Excel 2007

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 from the LNK files and jump lists refute this claim. The file's last access time is 3/2/2014 18:45.

10) 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 from the LNK files and jump lists refute this claim. The last access time on the removable storage E: drive is on 3/2/2014 at 5:00.

11) 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 are helpful in a forensic investigation to identify the validity of statements regarding last access times, last modified times, and the time of creation for files. They are also useful for identifying this information of deleted files or files attached to an external drive. They both have similar functions to identify recent files on a drive.

12) When was "Personal.docx" sent to the Recycle Bin? (2 pts)

03/02/2014 18:51:16

13) When was "Clients.xlsx" sent to the Recycle Bin? (2 pts)

03/02/2014 18:51:16

14) Where was "Clients.xlsx" stored (full path) before being sent to the Recycle Bin? (2 pts)

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

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

402107 bytes

16) 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 is the name in the recycle bin for "2013Sales.xlsx.

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

There are 2 user accounts with files in the recycle bin.

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

The recycle bin is helpful in a forensic investigation because it can identify files that have been fully deleted. The recycle bin stores information on which files were deleted and where they were located for each user.

Analyze the registry hives and determine:

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

Windows 7 Service Pack 1

20) When was the operating system installed? (2 pts)

08/04/2012 13:21:00

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

VMware Tools, VMware user process, and MSC are configured to start each time the system boots.

22) How many USB storage devices have been connected to the system and what is the serial number of each USB device? (4 pts)

There are 2 USB storage devices connected to the system.

USBSTOR\Disk&Ven_Kingston&Prod_DT_101_G2&Rev_PMAP\0013729B678DEB20C51F0216&0

USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Micro&Rev_8.02\4859701DEF10326C&0

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

The names of the user accounts are Administrator, Guest, Win7, and Josh.

24) Which user accounts password protected? (2 pts)

Administrator, Win7, and Josh.

25) What is the name of the program executed on 1/5/2013 from a user's desktop? (2 pts)
C:\Users\Win7\Desktop\X12-30307.exe

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

http://skydrive.com/

http://dropbox.com/

http://outlook.com/

http://www.bing.com/

http://louisville.edu/

http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&cad=rja&ved=0CCYQFjAB&url=http%3A%2F%2Fwww.gocards.com%2F&ei=SYUTU9esL8ThyQGrv4GQDA&usg=AFQjCNFurxbow5xoyb4ZLikEoAZOXAhu3Q&bvm=bv.62286460,d.aWc

https://www.google.com/

http://www.amazon.com/

http://www.overstock.com/

http://google.com/

http://go.microsoft.com/fwlink/?LinkId=69157

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

03/02/2014 19:25:17

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

ACME-WORKSTATIO

29) 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)

Yes, the computer name has been changed. The initial computer name does not match the default name on the install date.

30) How many times has the "Win7" user logged in? (2 pts)

11 times.

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

Registry analysis can be helpful in an investigation because it can attach important information such as accessed files and exact times associate them with a user. You use this information to find any suspecting information with the registry.

Analyze the scheduled tasks and determine:

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

Each day

33) When is the "dkfo4f" scheduled task configured to execute? (2 pts)

At log in

34) When was the "dkfo4f" create and what account was it created by? (2 pts)

2013-06-20 11:28:50 Guest

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

Yes, the schedule tasks were not created by a password protected account.

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

36) What is the user name of the account that sent "Manna.doc" to the Recycle Bin? How did you determine this? (5 pts)

Josh is the user that sent Manna.doc to the recycle bin which I found using the SID.

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

WIN-lpue2oj805q is the original computer name. I determined this using the dkfo4f tasks.

38) 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)

Rich.pdf was opened on the Kingston&Prod_DT_101_G2 USB Drive. serial number of the device is 0013729B678DEB20C51F0216&0. His can be determined using USBStor in the system hive.

39) 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)

Windows 10 OS
Windows Surface Pro 4
Registry Explorer
FTK Imager
CMD
LECmd
JLECmd
RegRipper