**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: a flash drive or Hard Drive.**

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

**3/2/2014 18:45:00**

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

**E: flash drive or hard drive**

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

**3/2/2014 18:50:12**

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**

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)

**It isn’t true because the evidence shows he still accessed the file on 3/2/2014 on the target accessed.**

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)

**It isn’t true because the evidence shows he accessed it on 3/2/2014 5:00:00**

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

**A link list is important to an investigation because it shows each time a file is opened or accessed.**

**Analyze the Recycle Bin and determine:**

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

**3/2/2014 18:51:16**

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

**3/2/2014 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**

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.xlsx**

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

**1 - Win7**

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

**The recycle bin analysis is helpful in a forensic investigation because it shows all the files that were deleted, dates, and what user deleted those files.**

**Analyze the registry hives and determine:**

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

**Windows 7 Professional Service Pack 1**

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

**Tue Jul 14 04:53:25 2009**

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

**VMwareTray.exe, vmtoolsd.exe, and msseces.exe**

22) How many USB storage devices have been connected to the system and what is the serial

number of each USB device? (4 pts)

**2**

1. **Prod\_DT\_101\_G2&amp;Rev\_PMAP#0013729B678DEB20C51F0216&0**
2. **Prod\_Cruzer\_Micro&amp;Rev\_8.02#4859701DEF10326C0**

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

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

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

**Administrator, 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 (3)**

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

**#1 - http://skydrive.com/**

**#2 - http://dropbox.com/**

**#3 - http://outlook.com/**

**#4 - http://www.bing.com/**

**#5 - http://louisville.edu/**

**#6 - http://www.google.com/url?sa=t&amp;rct=j&amp;q=&amp;esrc=s&amp;frm=1&amp;source=web&amp;cd=2&amp;cad=rja&amp;**

**ved=0CCYQFjAB&amp;url=http%3A%2F%2Fwww.gocards.com%2F&amp;ei=SYUTU9esL8ThyQGrv4G**

**QDA&amp;usg=AFQjCNFurxbow5xoyb4ZLikEoAZOXAhu3Q&amp;bvm=bv.62286460,d.aWc**

**#7 - https://www.google.com/**

**#8 - http://www.amazon.com/**

**#9 - http://www.overstock.com/**

**#10 - http://google.com/**

**#11 - http://go.microsoft.com/fwlink/?LinkId=69157**

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

**Sun Mar 2 19:25:17 2014 (UTC)**

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)

**The computer has changed from MNMSRVC to ACME-WORKSTATIO. This was changed on March 2, 2014 at 19:26:43. I determined this by looking at the Last Write Date.**

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

**11**

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

**Registers hold large amounts of information about the computer, the system, and the different user accounts on the computer. This will show what user had access to certain files.**

**Analyze the scheduled tasks and determine:**

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

**Every Other Day**

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

**when WIN 7 user logs in**

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

**Guest Account on June 20, 2013 at 11:28:50**

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

**Yes, ‘dkfo4f’ is created by the Guest Account and runs whenever the Win7 account is logged on.**

**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 sent the file to the recycle bin. I looked at the SID in the recycle bin and compared it to the profile list in registry explorer to find the user name.**

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

**The Original Computer Name is WIN-LPUE2OJ805Q. I found this under the dkfo4f task when viewing it in FTK Imager to find it.**

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)

**Manufacture: SanDisk**

**Model: Cruzer Micro**

**Serial Number: 4859701DEF10326C&0**

**I determined this by checking the rich file in LECmd and found the E:\ drive it was on. Then I compared it in RegExplorer where I looked at the SYSTEM hive and checked under mounted devices.**

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, FTK Imager, LECmd, JLECmd, RegRipper**