Paige Fenwick

CIS 484-75

Jason Hale

# Project 3

1.

a) The full path when the excel file was last opened was C:\Users\Win7\Documents\2013-Sales.xlsx.
b) It was accessed from a removable storage disk, more specifically a USB device. This is found underneath the link information in the Volume Information section after using the LECmd command.
c) The '2013 list for Dave' file was last opened on March 02 2014 at 5:00:00 AM.
d) The file was accessed from a removable device called MY STUFF. I determined this by using the JumpLister and looking at the Drive type.
e) The last modified time is 3/2/2014 at 6:50:12 PM.
f) The device serial number is B4A2B40D and is a removable storage disk, mostly likely a USB. This is why we can determine the serial number from LECmd.
g) Microsoft Office 2007 because the file is an xlsx file format.
h) The full path when the document was last opened was C:\Users\Win7\Documents\Personal.docx
i) The evidence would refute this claim because from the Source file information and header information, we can see that the source and target modified dates are on 3/2/2014, which is the day after 3/1/2014.
j) The evidence from the LNK files would also refute this claim because we can see that the files were connected and modified on 3/2/2014, which is the day after 3/1/2014.
k) LNK and jump files can be useful in an investigation because the files can offer a variety of information, from last modified times, last accessed times and the device the files were stored on. This can provide a detail look into how the owner behaves and interacts with their system.

2.

a) The Personal document was sent to the recycle bin at 3/2/2014 at 14:15:16 EST.
b) The Clients excel file was sent to the recycle bin at 3/2/2014 at 14:51:16 EST.
c) Before being sent to the recycle bin, the clients excel file was stored at C:\Users\Win7\Documents\Clients.xlsx.
d) The size in bytes of the Tax Breaks PDF is 402107.
e) The name of the file in the recycle bin is $IWN9JUT. I determined this by using the Recycling Parser to find the file name and file path.
f) Yes, there are two different users sending items to the recycle bin. We know this because their SID id numbers are listed as folders with their deleted files being stored within those folders.
g) By analyzing the recycling bin, we can determine how many users are deleting items and what items they are deleting. This is useful in understanding how many people have

access to these files and how exactly they are interacting with them at given points in time.

3.

a) On the system, the operating system is the Windows 7 Professional and the service pack installed is Service Pack 1.
b) The operating system was installed on July 14th 2009 at 12:53:25 EST.
c) There are three programs that are configured to start at run time: MSC, VMWare tools and VMWare User Process.
d) There were two USB storage devices connected to the system.
    i. Their serial numbers are as follows: 0013729B678DEB20C51F0216&0 and 4859701DEF10326C&0.
e) The user accounts on the system are Administrator, Guest, Josh and Win7. HomeGroupUser is also listed but seems to have been deleted.
f) Yes Administrator, Win7 and Josh are all password protected accounts.
g) The program that was opened on that date was Microsoft Word 2007. This can be found by looking at the LNK icon.
h) The following url's were typed into the address bar: http://skydrive.com/, http://google.com/, http://go.mircosoft.com/fwlink/?LinkId=69157, http://dropbox.com, http://outlook.com/, http://www.bing.com/, http://louisvill.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, http://www.google.com/, http://www.amazon.com/ and http://www.overstock.com/.
    i. The most recently typed URL was http://skydrive.com/.
i) The name of the computer is ACME-WORKSTATIO.
    i. The computer name has changed because the OS was installed in 2009 and the last updated computer name was shown to be updated at 3/2/2013.
j) The Win7 user logged in 11 times.
k) By using and understanding registry analysis, we can find out found important user information and other valuable facts about the computer. This can help us to better understand exactly how the user uses the system and more importantly, there most recently accessed programs and files which will give answers to questions during a forensic analysis.

4.

a) The Google update is scheduled to execute at every logon and once every day. We know this by opening the update in XML Notepad and viewing the enabled triggers.
b) The dkfo4f is scheduled to execute at every logon. We know this because in XML Notepad, this is the only enabled trigger for dkfo4f.
c) The dkfo4f was created on 6/20/2013 at 11:28:50 and it was created by the Guest user. We know this because within XML Notepad, we can view the author information and find who was logged in at the specific time the scheduled task was created.
d) The scheduled task dkfo4f seems suspicious because it was installed by a Guest user account and schedule tasks should be installed by Administrator accounts only.

5.

a) Josh is the user that deleted the Manna doc. This can be discovered by using the Recycle Bin Parse application to determine the name of the document that is found in the folder labeled by a specific SID id. We can then use the Registry Explorer to compare the SID id to the users that are listed on the system. Once we match the SID id we can conclude that Josh deleted the file.
b) The original computer name was mnmsrvc. This can be found by looking in the Registry Explorer.
c) The manufacturer is SanDisk&Prod, the model is Cruzer_Micro&Rev_8.02 and the serial number is 4859701DEF10326C&0. To find this, I determined the name of the removable drive by using LECmd. Then, using Registry Explorer, I used the EMDMgmt Key to match the friendly name I found in LECmd and then looked in the folder name to find the manufacturer, model and serial number.

6.

**Hardware:**

- Lenovo Think Pad

**Software:**

- FTK Imager
- Windows 7 OS
- E01 File Image
- Command Line
- LECmd.exe
- Registry Explorer v0.7.1.0
- XML Notepad
- JumpLister
- WinHex
- Notepad
- Windows Recycle Bin $I File Parser
- RegRipper