Windows 8 Forensics

Windows 8 Forensics

Ethan Fleisher

Senator Patrick Leahy Center for Digital Investigation

Overview

Today I am starting the preliminary research on the Windows 8 Operating System from a Digital Forensics standpoint. I will be comparing it primarily to known information on the Windows 7 Operating System. There are going to be many items that I am looking at, and any comments with suggestions for further things to look into would be appreciated. Topics so far include:

- Recycle Bin Properties
- USB Drive Activity
- Internet History
- Windows 8 Reset and Reload Feature
- Event Logs
- Prefetch Files
- Jump Lists
- File History Feature

As I dig into these topics, there is likely to be a large amount of information that will be discovered. It is important to remember, though, that some of these topics may yield little to no differences.

Purpose

The purpose of this project is to determine key differences between the Windows 7 and Windows 8 operating system from a forensic standpoint in order to determine if there are any significant changes that will be either beneficial or detrimental to the forensic investigation process.

Version:1.0 StartHTML:0000000167 EndHTML:0000003071 StartFragment:0000000747 EndFragment:0000003055 Version:1.0 StartHTML:0000000167 EndHTML:0000002862 StartFragment:0000000747 EndFragment:0000002846

Preliminary Tool List

1.

Encase 6.19 Law Enforcement Edition -

http://www.guidancesoftware.com/forensic.htm

1.

Forensic ToolKit Imager 3.0 -

Windows 8 Forensics

http://accessdata.com/support/adownloads

1.

Forensic ToolKit 1.81.6 -

http://accessdata.com/support/adownloads

1.

Mandiant Web Historian -

http://www.mandiant.com/products/free_software/web_historian/

1.

Net Analysis -

http://www.digital-detective.co.uk/netanalysis.asp

1.

DCode -

http://www.digital-detective.co.uk/freetools/decode.asp

1.

RegDecoder -

http://www.digitalforensicssolutions.com/registrydecoder/

1.

Internet Evidence Finder -

http://www.jadsoftware.com/?page_id=1083

Recycle Bin Properties

With this part, I am testing the recycle bin properties of Windows 8 to see how they compare to Windows 7. In Windows 8, the Recycle bin, using forensics tools, consists of $Recycle.Bin, $R, and $I files.

1. Created “I wonder if this will appear“ at 10:14

Deleted “I wonder if this will appear“ at 10:14

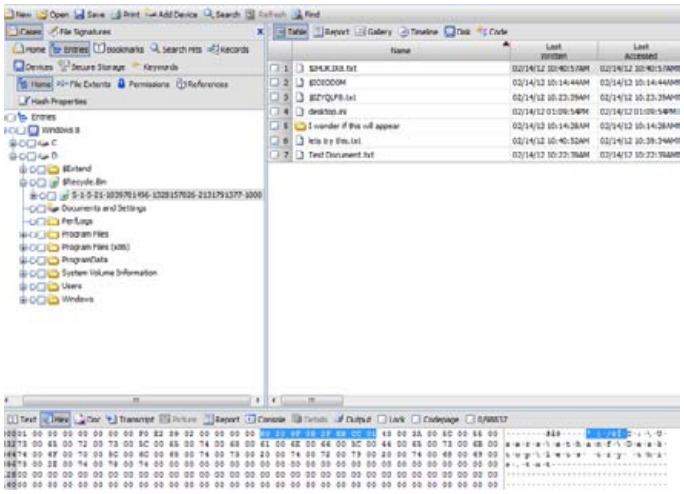
1. Created “test document.txt“ at 10:22

Deleted “test document.txt“ at 10:23

1. Created “lets try this” at 10:40 – filled it with text, 36.5 mb

Deleted “lets try this“ at 10:40

Recycle Bin in EnCase still has $Recycle.Bin and $I files. There are still $R files, but they do not show up directly in the $Recycle.Bin folder.



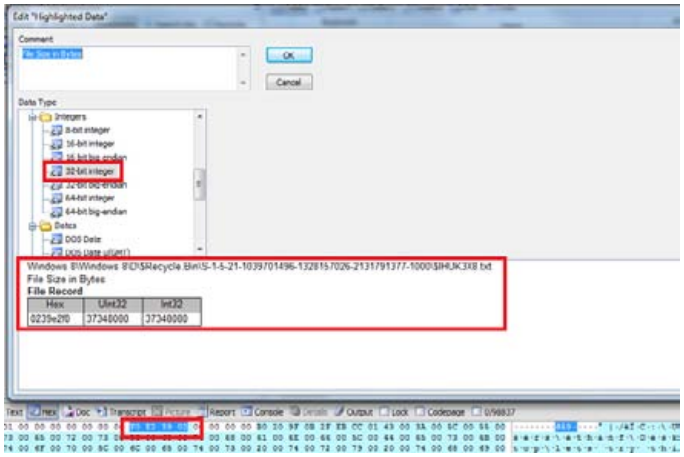
Windows 8 Forensics

Located and verified times of “test document”, “lets try this”, and “I wonder if this will appear” to be accurate to what I recorded when creating/deleting originally.

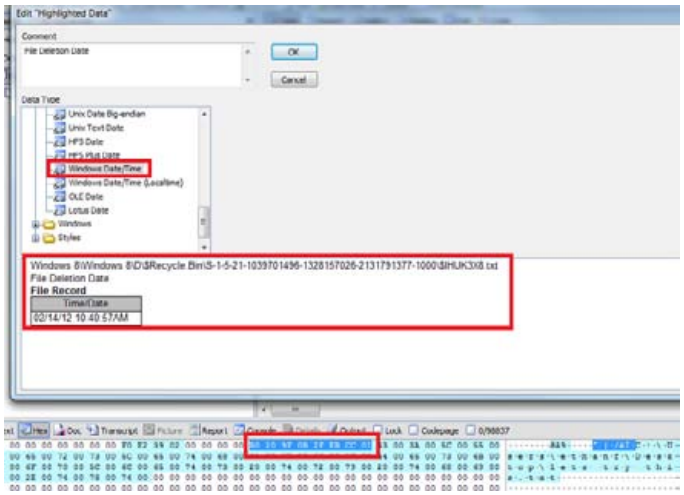
Verified hex values for $I files in comparison to known Windows 7 values.

Bytes 0-7 are still the file header, always 01 followed by seven sets of 00.

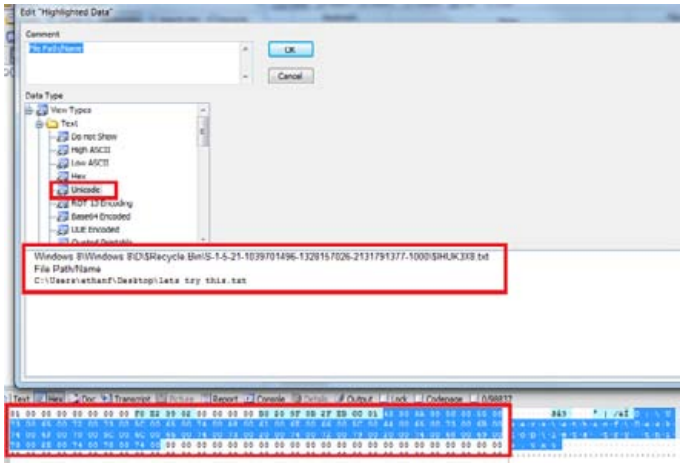
Bytes 8-15 are the original file size, stored in hex, in little-endian. This can be converted into big endian format and converted with a hex calculator to a decimal notation to determine the size in bytes. I tested this with the “Lets try this” document that was 36.5mb. The hex value in encase was F0 E2 39 02, read in little endian. Converting this into big endian yields 02 39 E2 F0, which ran through a hex calculator shows that it is 37348080 bytes, which is roughly 36.5mb



Bytes 16-23 reflect the deleted date time stamp, represented per normal standards (number of seconds since Midnight, January 1, 1601).



Bytes 24-543 reflect the original file path/name.



The next step in the process

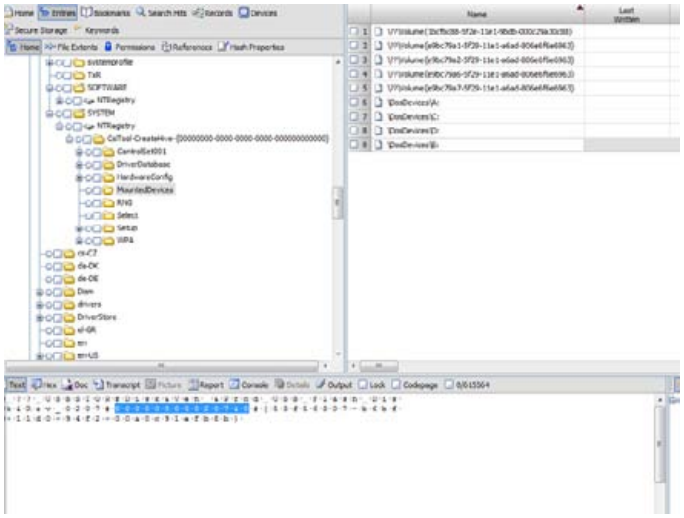
USB Drive Activity

To start with Windows 8 USB drive forensics, I assumed it would be pretty similar to Windows 7. I booted up a fresh new Windows 8 VM and plugged a thumb drive into my local system. Like normal, the VM recognized it as it should. At this point I shut the VM down and opened it up in EnCase to look at what was happening. Most of the findings

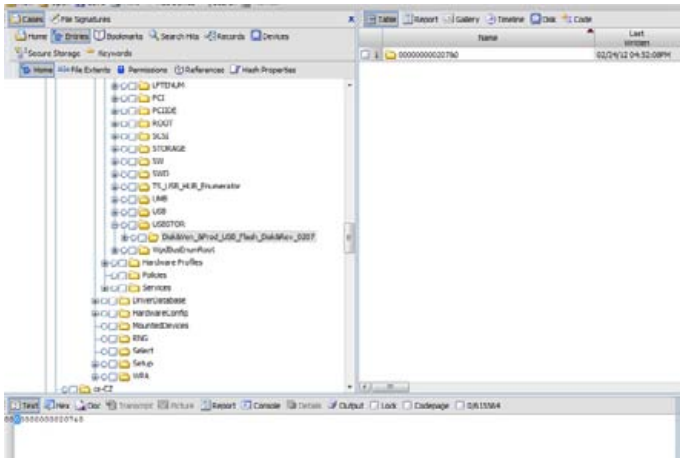
Windows 8 Forensics

were pretty similar to Windows 7 USB forensics. For example,

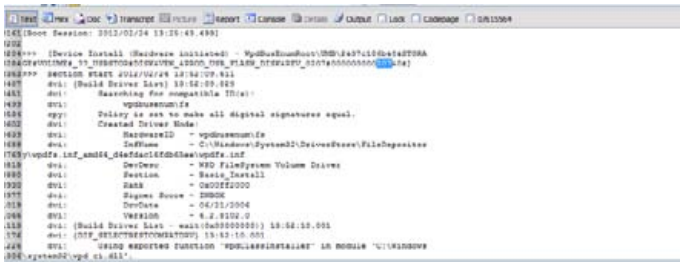
Mounted devices tab:



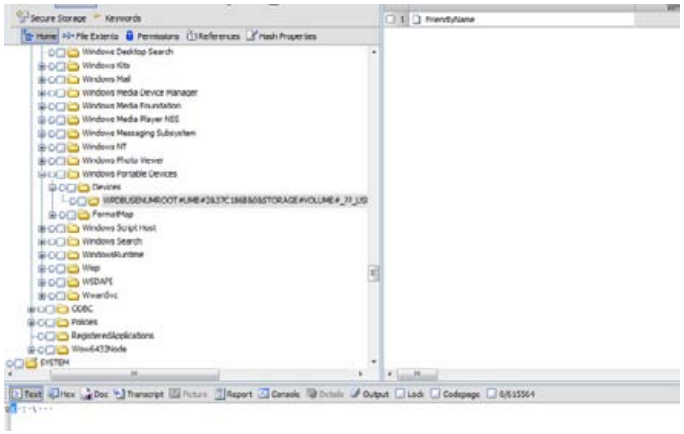
System\currentcontrol\enum\usbstor:



Setupapi.dev.log:



Software\microsoft\windows portable devices\devices – friendly name link:



This shows that forensics of USB thumb drives in Windows 8 is very similar to Windows 7 forensics. There may be new potential keys that are created, but for what is necessary to prove that a thumb drive was plugged into a system and when it was first plugged in, this is necessary.

For the next part of this project click here: Windows 8 Forensics Part 2

Windows 8 Forensics

If you have any comments, questions and/or suggestion please feel free to leave a comment here on the blog. Or feel free to email us atLCDI@champlain.edu, with «Windows 8 Forensics» in the subject.