Super Timeline

Written by
Dan Doonan
Researched by
Jacob Blend and Dan Doonan

The Senator Patrick Leahy Center for Digital Investigation

Champlain College

Date (April 11, 2013)

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

A detailed timeline of everything that occurred on a system, also known as a Super Timeline, can be extremely beneficial in determining what took place in a digital investigation. It can provide specific dates and times of when files are created and/or deleted, when programs were ran, when removable media was connected, etc.

Manually creating a timeline which included this information would be difficult and extremely time consuming. Not only would you need to copy down the timestamps for every file on the system, you would also need to understand how every application stores its data, such as such as the history files for web browsers.

Fortunately the log2timeline tool designed by Kristinn Guðjónsson was programmed to automatically create these timelines.

Research Questions

- Is creating a Super Timeline using log2timeline difficult?
- Is it difficult to analyze this timeline?
- Are there methods which exist to aid in analyzing the timeline?

Prior Work

There has been prior work on the subject such as Kristinn Guðjónsson's paper "Mastering the Super Timeline with log2timeline," which outlines in specific detail what the tool does and how it works. Rob Lee's blog post "Digital Forensic SIFTing: SUPER Timeline Creation using log2timeline-sift" explains how to use log2timeline to create a super timeline on the SIFT Workstation. The log2timeline cheat sheet created by David Nides is another good reference for using the tool.

Methodology and Methods

Overarching Methodology

To conduct our research, we generated user activity on a fresh install of Windows 7 on a spare XPS workstation (the full specifications of the machine can be seen in Table 2). A detailed log of the activity was kept and can be seen in Table 1.

Data Collection

The machine's hard drive was then removed, and an .E01 forensic image was created using FTK Imager. The .E01 image was then converted into the .dd and placed into the SIFT Workstation. The Sift Workstation was used because of its cost (free) and because it already include the log2timeline tool. The image was converted to the .dd format due to difficulties with mounting the .E01.

Analysis

The .dd image was then brought into the SIFT Workstation by placing it into a VMWare shared folder. The log2timeline-sift command was run against the image to automatically generate a timeline using every available data source that log2timeline is able to parse, as shown in Figure 1. The output of this command was saved into a .txt file.

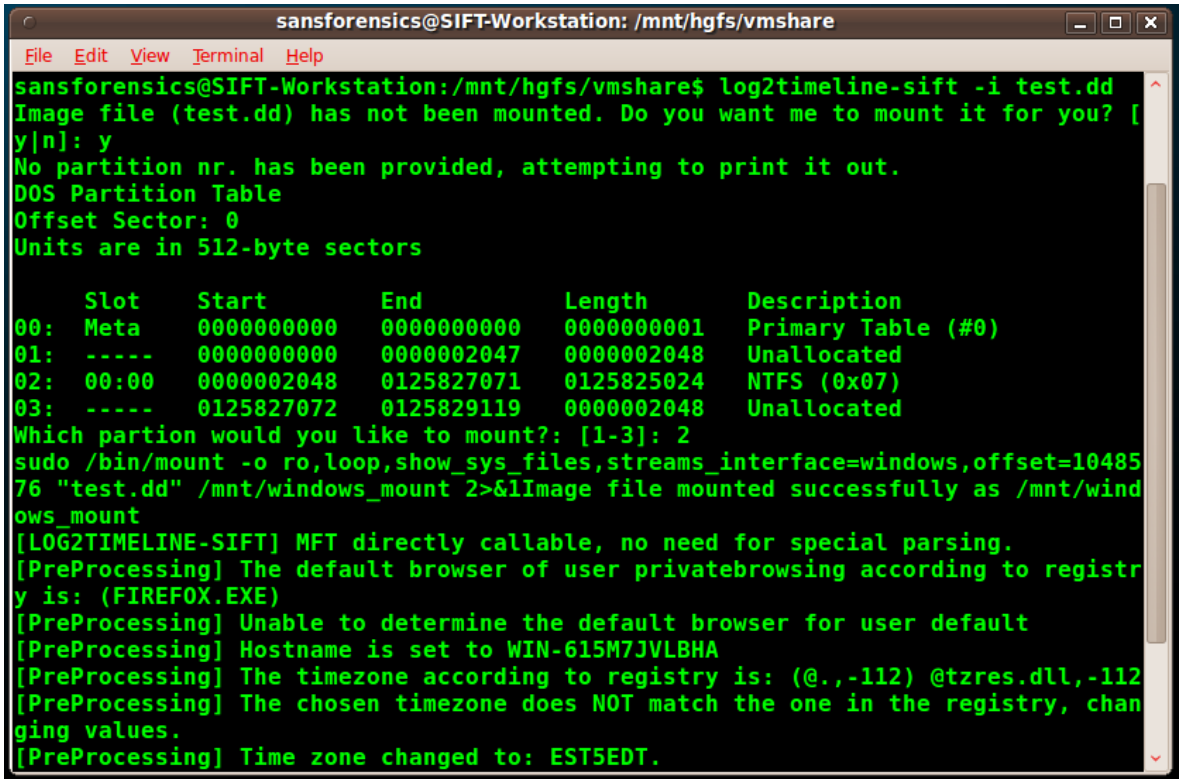


Figure 1 - log2timeline-sift

The l2t_process command was then used (shown in Figure 2) to filter the .txt file by the date range, including the user activity. The output of this command was saved into a .csv file.

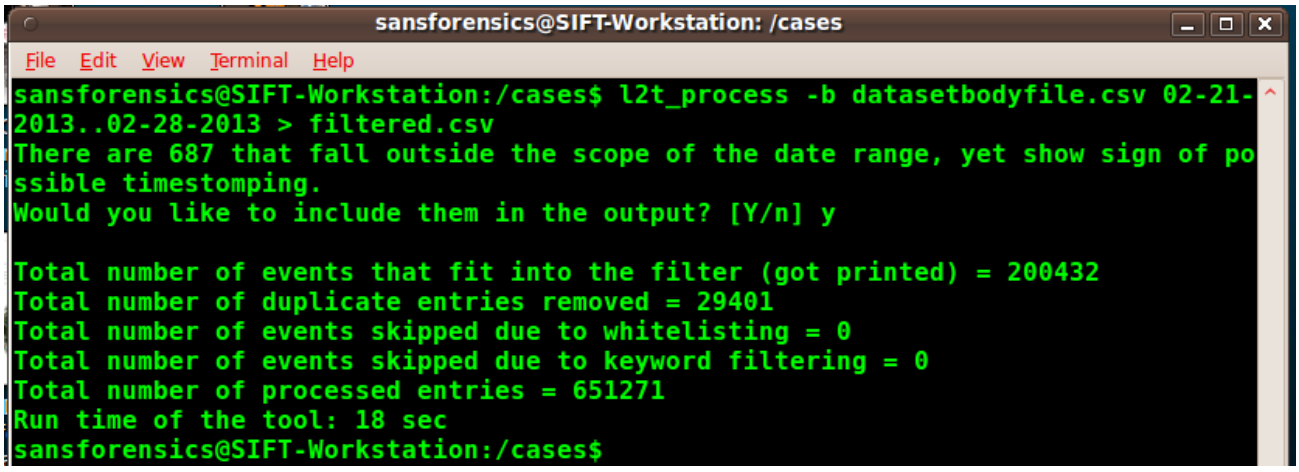


Figure 2 - l2t_process

Excel

The .csv file created by the l2t_process was then opened in Microsoft Excel. Initially there was an overwhelming amount of information but with the sort and search functions built into Excel, it became easier to filter through it.

The sort function (Figure 4) of Excel made it manageable to sort through the spreadsheet by date and time. It was sorted first by date from oldest to newest, then time from smallest to largest. The search function (Figure 3) made finding the specific times at which user activity occurred simple, as you can search for the specific date or time.

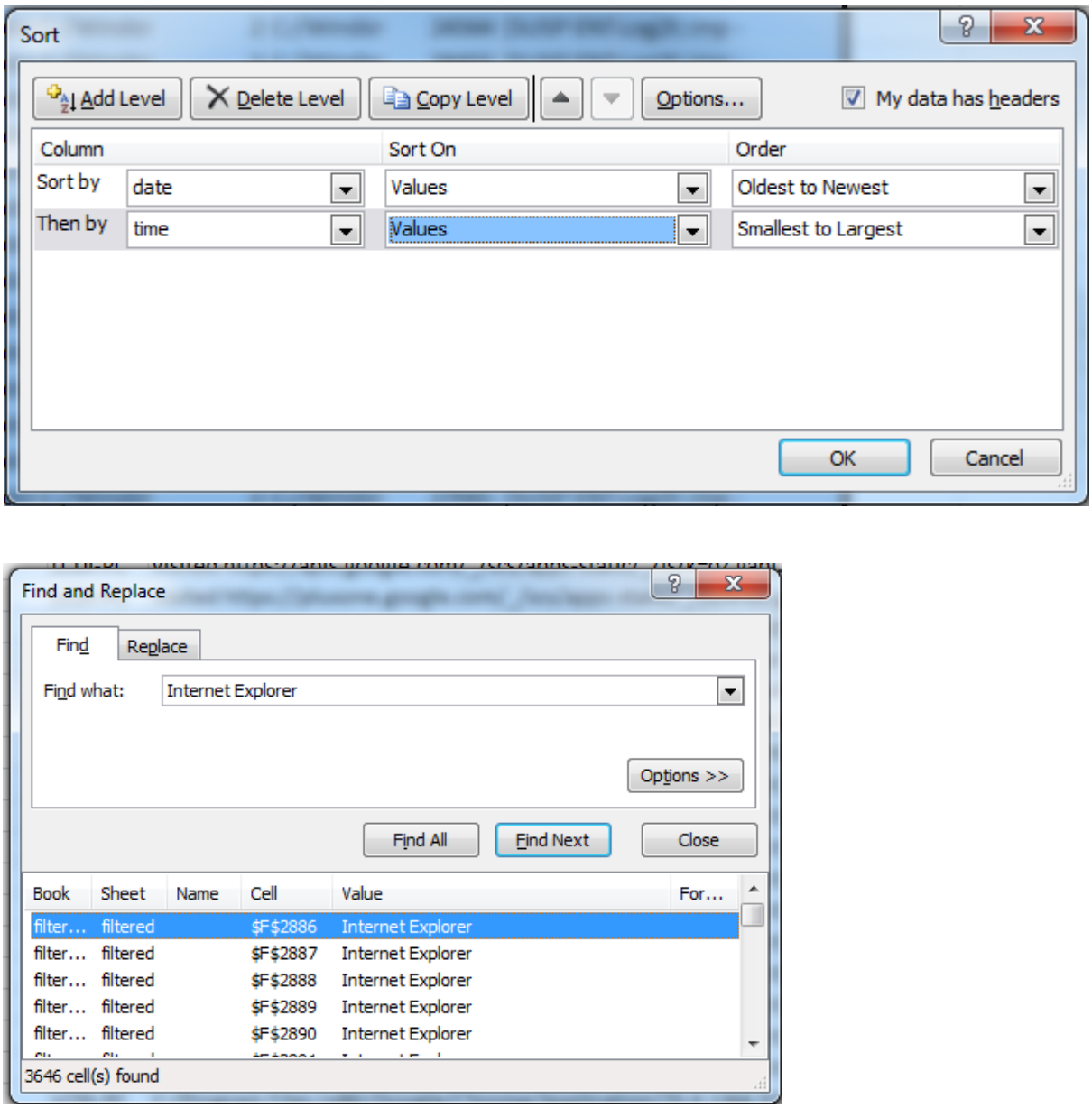


Figure 3 - Excel Search Function

4n6time

4n6time created by David Nides "...is a free, cross-platform forensic tool for timeline creation and review" (plaso). This tool does an excellent job of searching and sorting through the timeline created by log2timeline.

In order to use this tool, the .csv file created by the l2t_process must be converted into a SQLite database.

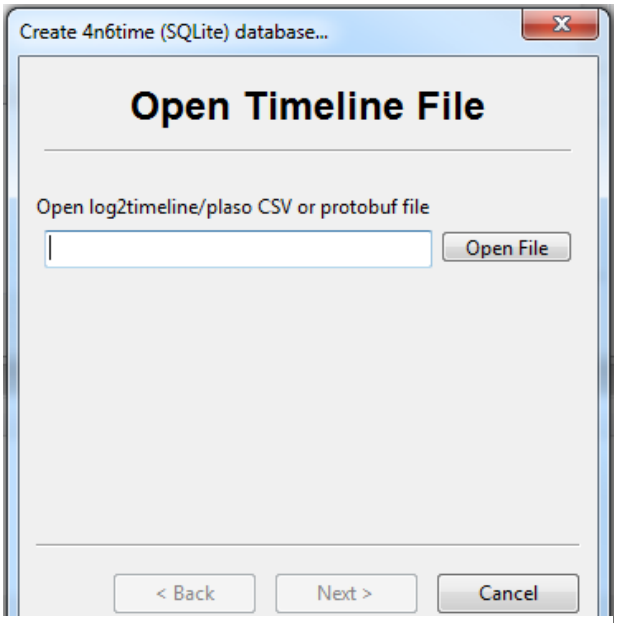


Figure 5 - Selecting the log2timline CSV

4n6time is capable of converting the file via File -> Create Database. This will open a wizard which will first prompt you to open the log2timeine .csv file. The next page will prompt you for the location to save the database. It will then present options for date filters and index fields.

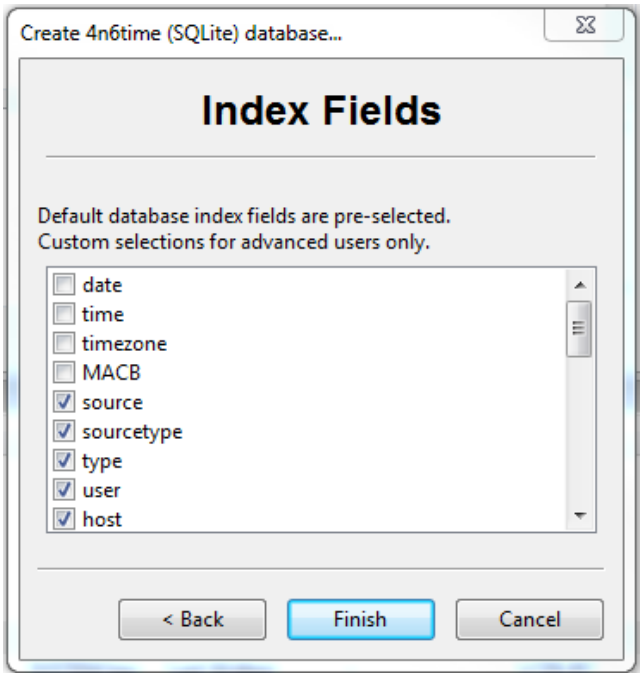


Figure 6 - Index Fields

The database will then be opened in 4n6time, which will present options to search and filter the database. Options include Host, User, SourceType, Data and Time, and a String Search.

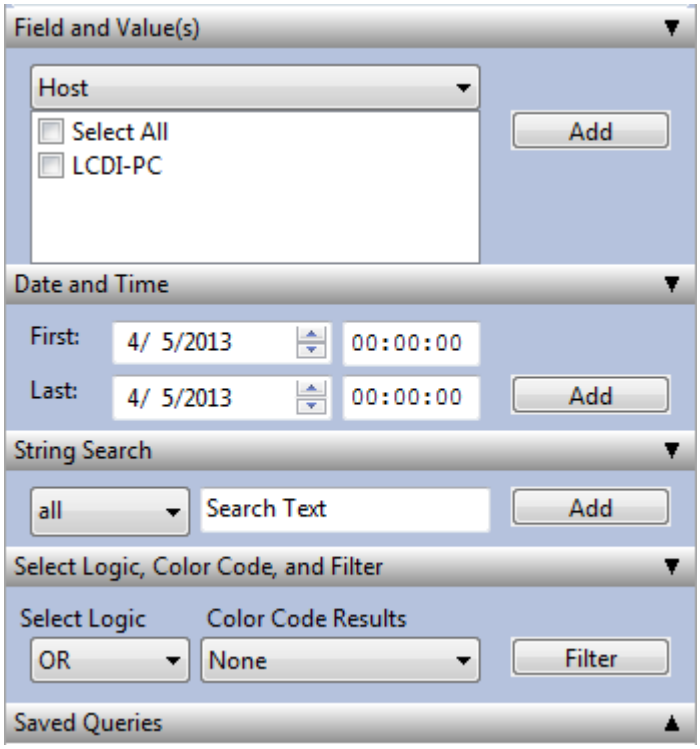
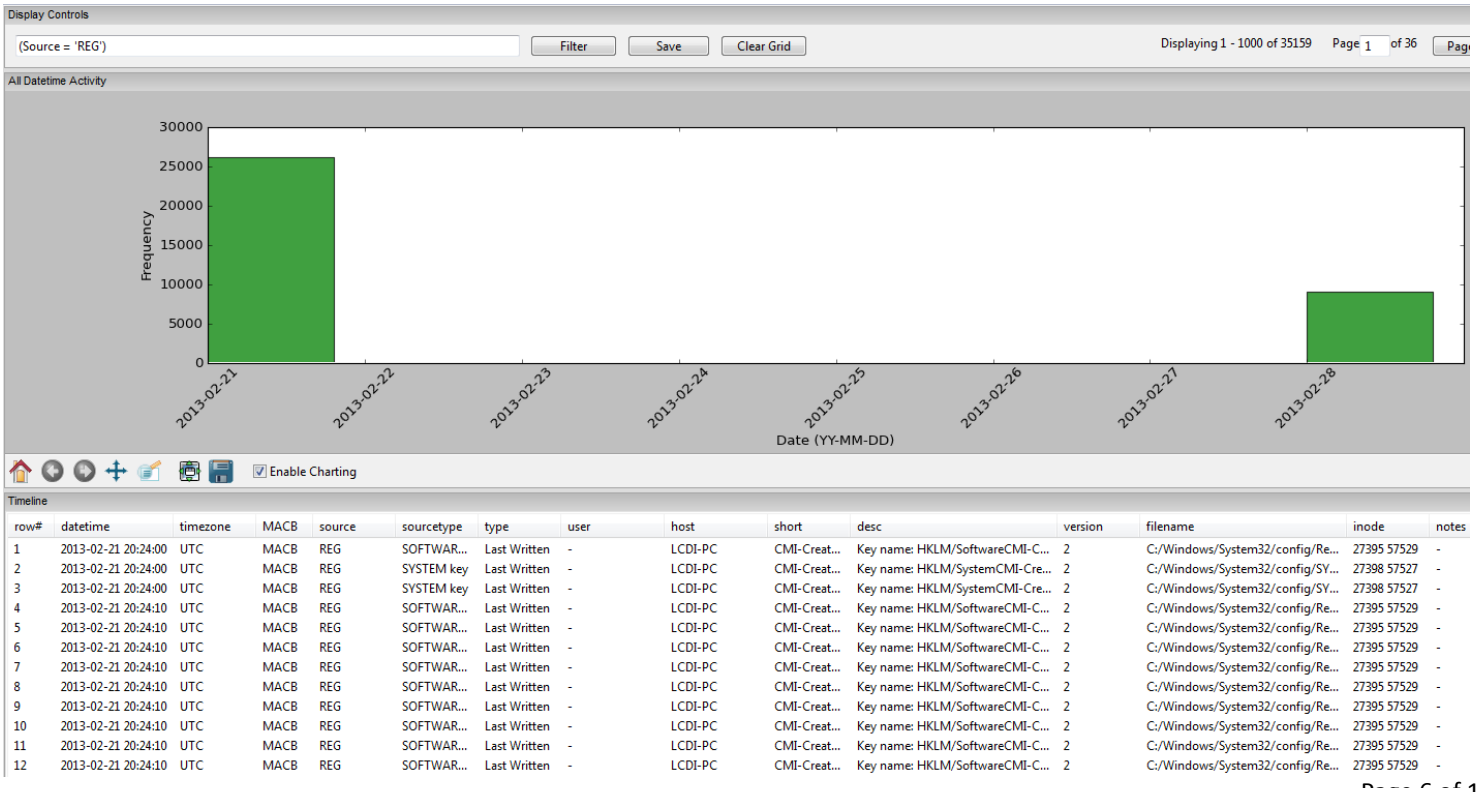


Figure 7 – 4n6time Filters

Once the filter criteria have been selected and applied, 4n6time will display the individual results below a bar graph that displays the frequency of the results on each specific date.



row#	datetime	timezone	MACB	source	sourcetype	type	user	host	short	desc	version	filename	inode	notes
1	2013-02-21 20:24:00	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
2	2013-02-21 20:24:00	UTC	MACB	REG	SYSTEM key	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SystemCMI-Cre...	2	C:/Windows/System32/config/SY...	27398 57527	-
3	2013-02-21 20:24:00	UTC	MACB	REG	SYSTEM key	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SystemCMI-Cre...	2	C:/Windows/System32/config/SY...	27398 57527	-
4	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
5	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
6	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
7	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
8	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
9	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
10	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
11	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-
12	2013-02-21 20:24:10	UTC	MACB	REG	SOFTWAR...	Last Written	-	LCDI-PC	CMI-Creat...	Key name: HKLM/SoftwareCMI-C...	2	C:/Windows/System32/config/Re...	27395 57529	-

Figure 8 - 4n6time Results

Results

Chrome

Chrome web history does not list the specific URL of websites visited; it only lists the creation and modification or various cache files. For sites that include Flash content, the URL of the site can be seen as Flash cookies and cache files are created such as, “Flash Cookie: site skype.com/settings.” These entries were found for Skype.com and cnn.com, and examples can be seen in Figure 9 and the correlating log entries can be seen in Figure 10.

C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/9N4PLZKA/skype.com
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00002a
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/6AA3321A15A787985201D7A6820782F0_0AB46376AFB6F40B0426680E3025D384
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/9N4PLZKA
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/6AA3321A15A787985201D7A6820782F0_0AB46376AFB6F40B0426680E3025D384
Flash Cookie: site skype.com/settings
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/BD8A14C7C024625432CC03FE72E47EF0_D6CE585A0142F6FC2E8BA6CCD6EC6CBE
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000025
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/9N4PLZKA/macromedia.co
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000026
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/BD8A14C7C024625432CC03FE72E47EF0_D6CE585A0142F6FC2E8BA6CCD6EC6CBE
Flash Cookie: site settings
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000024
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000029
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/9N4PLZKA/skype.com/#ui
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/9N4PLZKA/skype.com/#use
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/9N4PLZKA/macromedia.co
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00002c
C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00002d

Figure 9 - Chrome Results

2/21/2013	15:32:10	CNN.com
2/21/2013	3:33:00 PM	Skype.com

Figure 10 - Chrome Activity Log

Internet Explorer

Internet Explorer history can be easily found by searching for ‘Internet Explorer’ under source type. Each entry will list the date, time, user account, and the URL that was visited. An example can be seen below in Figure 11, and the related log entry can be seen in Figure 12.

2/21/2013	20:28:19	UTC	MACB	WEBHIST	Internet Explorer	Website modified cooki	Cookie:lcc	LCDI-PC	visited www.msn.com/

Figure 11 - Internet Explorer Results

2/21/2013	3:27:06 PM	Opened Internet Explorer 8	Opened with MSN.com homepage

Figure 12 - Internet Explorer Log

Skype

Entries were found that show Skype was installed to the system. The Skype installer can be seen in the Downloads directory (Figure 13), and then a large amount of registry keys being created and updated reference Skype. Figure 14 shows the related entry from the activity log.

2/21/2013	20:33:29	UTC	MACB	FILE	NTFS $MFT	$SI [MACB] time	-	LCDI-PC	C:/Users/LCDI/Downloads/SkypeSetup.exe

Figure 13 - Skype Results

2/21/2013	3:33:35 PM	started download

Figure 14 - Skype Log

USB Flash Drive

There are a series of entries relating to registry keys being created and modified around the time that the USB Flash Drive was inserted into the workstation. One of the entries includes a reference to the exact manufacture and model of the flash drive and can be seen in Figure 15, while the related log entry is visible in Figure 16.

20:43:32	UTC	..C.	FILE	NTFS $MFT	C:/Windows/System32/drivers/USBSTOR.SYS
20:43:33	UTC	MACB	REG	SYSTEM key	CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}/ControlSet001/Enum/USB/VID_0781&PID_5575/4C532000010908118205/P
20:43:33	UTC	MACB	REG	SYSTEM key	CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}/ControlSet001/Enum/USBSTOR/Disk&Ven_SanDisk&Prod_Cruzer_Glide&
20:43:33	UTC	MACB	REG	SYSTEM key	CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}/ControlSet002/Enum/USB/VID_0781&PID_5575/4C532000010908118205/P
20:43:33	UTC	MACB	REG	SYSTEM key	CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}/ControlSet002/Control/DeviceClasses/{a5dcbf10-6530-11d2-901f-00c04fb
20:43:33	UTC	MACB	REG	SYSTEM key	CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}/ControlSet002/Enum/USBSTOR/Disk&Ven_SanDisk&Prod_Cruzer_Glide&
20:43:33	UTC	MACB	REG	SYSTEM key	CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}/ControlSet001/Enum/USBSTOR/Disk&Ven_SanDisk&Prod_Cruzer_Glide&

Figure 15 - USB Drive Results

2/21/2013	3:43:30 PM	Inserted USB Flash drive

Figure 16 - USB Activity Log

Text Document

There are a series of entries relating to the .txt document that show the file being created, opened in notepad.exe, and modified. The first related entry shows the file being created and includes the full path to the file, as shown in Figure 17. This entry includes the updated name of the file, rather than the name the file was created with.

The following entries in Figure 17 show the file being opened, such as ‘visited file:///C:/Users/LCDI/Desktop/forensics.txt’. There are also entries from the registry recent documents key that include ‘Recently opened file of extension: .txt - value: forensics.txt.’ At the same time, the UserAssist key is updated to show that notepad.exe was opened. Figure 18 shows the logged dates and times for when this document was created.

2/21/2013	20:45:25	UTC	.A.B	FILE	NTFS $MFT	C:/Users/LCDI/Desktop/forensics.txt
2/21/2013	20:45:25	UTC	.A..	LNK	Shortcut LNK	C:/Users/
2/21/2013	20:45:25	UTC	..CB	LNK	Shortcut LNK	C:/Users/
2/21/2013	20:45:25	UTC	M...	LNK	Shortcut LNK	C:/Users/
2/21/2013	20:46:10	UTC	MAC.	FILE	NTFS $MFT	C:/Users/LCDI/Desktop
2/21/2013	20:46:50	UTC	M.C.	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDes
2/21/2013	20:46:50	UTC	MACB	WEBHIST	Internet Explor	visited file:///C:/Users/LCDI/Desktop/forensics.txt
2/21/2013	20:46:50	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming/Microsoft/Windows/Recent/forensics.lnk
2/21/2013	20:46:50	UTC	MACB	WEBHIST	Internet Explor	visited file:///C:/Users/LCDI/Desktop/forensics.txt
2/21/2013	20:46:50	UTC	MACB	REG	FileExts key	File extension .txt opened by NOTEPAD.EXE

Figure 17 - Text Document Results

2/21/2013	3:45:25 PM	created .txt on desktop	
2/21/2013	3:46:10 PM	renamed forenscs	
2/21/2013	3:47:00 PM	edited document	put in 'super secret stuff'

Figure 18 - Text Document Log

Dropbox

Entries were found that show Dropbox was downloaded and installed on the system. An entry shows the creation of 'Dropbox 1.6.17.exe' in the downloads folder. The time this file was created matches the time that the file was downloaded on the log sheet, as shown in Figure 19. The next entries show a series of registry keys and files being created which relate to Dropbox, some of which can be seen in Figure 20.

2/21/2013	3:48:40 PM	clicked download	new webpage, download started

Figure 19 - Dropbox Log

2/21/2013	20:48:41	UTC	.A.B	FILE	NTFS $MFT	C:/Users/LCDI/Downloads/Dropbox 1.6.17.exe
2/21/2013	20:48:41	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Local/Google/Chrome/User Data/
2/21/2013	20:48:49	UTC	M.C.	FILE	NTFS $MFT	C:/Users/LCDI/Downloads/Dropbox 1.6.17.exe
2/21/2013	20:49:02	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlC
2/21/2013	20:49:02	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlC
2/21/2013	20:49:02	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlC
2/21/2013	20:49:02	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlC
2/21/2013	20:49:12	UTC	.A.B	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming/Dropbox/installer/l/512
2/21/2013	20:49:12	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming/Dropbox/installer/l
2/21/2013	20:49:12	UTC	...B	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming/Dropbox
2/21/2013	20:49:12	UTC	MAC.	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming
2/21/2013	20:49:12	UTC	MACB	FILE	NTFS $MFT	C:/Users/LCDI/AppData/Roaming/Dropbox/installer
2/21/2013	20:49:21	UTC	.A.B	FILE	NTFS $MFT	C:/Windows/Prefetch/DROPBOX 1.6.17.EXE-53B8A9ED.pf

Figure 20 - Dropbox Results

Gimp

Entries were found that show Gimp was downloaded and installed on the system. An entry shows the creation of 'gimp-2.8.4-setup.exe' in the downloads folder. The time this file was created matches the time that was logged. The following entries show a series of registry keys and files being created relating to Gimp that can be seen in Figure 21 and the related log entry in Figure 22.

C:/Users/LCDI/Downloads/gimp-2.8.4-setup.exe
C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.1.gthr
C:/Users/LCDI/Downloads
C:/Users/LCDI/Downloads/gimp-2.8.4-setup.exe
Software/Microsoft/Windows/CurrentVersion/Explorer/Discardable/PostSetup/ComponentCategories/{56FFC
CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}/Microsoft/SystemCertificates/AuthRoot/Certificate
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/BE432C2EE45E016635C9B13C029DA7E
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/BE432C2EE45E016635C9B13C029DA7E7
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/CE4CFAB51DB3F9AB265C1526D1E6F1
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/CE4CFAB51DB3F9AB265C1526D1E6F12
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/B1AA84065EC5876DF7F06B36A34A81
C:/Users/LCDI/AppData/LocalLow/Microsoft/CryptnetUrlCache/Content/B1AA84065EC5876DF7F06B36A34A8167
C:/Windows/Prefetch/CONSENT.EXE-531BD9EA.pf
C:/Windows/Prefetch/NVTRAY.EXE-DB83881B.pf
C:/Program Files/GIMP2~1/uninst/unins000.exe
C:/Users/LCDI/AppData/Local/Programs
C:/Users/LCDI/AppData/Local/Programs/Common
C:/Users/LCDI/AppData/Local
C:/Program Files/GIMP2~1/share/gimp/2.0/brushes/Media/Acrylic-04.gih
C:/Program Files/GIMP2~1/share/gimp/2.0/brushes/Texture/Texture-Hose-01.gih
C:/Program Files/GIMP2~1/share/gimp/2.0/gimpressionist/Brushes/crayon01.pgm

Figure 21 - Gimp Results

4:02:15 PM	clicked download gimp 2.8.4	
4:02:15 PM	brought to a sourceforge url where gimp auto downloaded	
16:03	Opened gimp setup	ran install
4:04:02 PM	install finished	

Figure 22 - Gimp Logs

User Account Activity

Log2timeline also parses registry keys from the SAM hive and will create entries that show when an account was created and how many times it has been logged in. It will also list the date and time of the last login for each account, as shown in Figure 23. The related log entry can be seen in Figure 24.

2/28/2013	21:14:25	UTC	.A..	REG	SAM key	Last Login	LCDI [1001]	LCDI-PC	count: 4

Figure 23 - User Account Activity

2/28/2013	4:14:00pm	logged in

Figure 24 - User Account Log

Conclusion

Creating a Super Timeline is made easy by the SIFT Workstation via the log2timeline-sift command. This command will automatically mount the image and prompt the user for the correct offset of the partition. It will then create a timeline which includes all the information that it can.

Analyzing the timeline can be overwhelming due to the large amount of information; however, the search and filter functions built into Excel can make this data manageable. 4n6time greatly streamlines the process of searching by providing more options and displaying the number of results in a bar graph. An advantage of Excel over 4n6time is that it will display the next chronological result rather than just the search hits.

/using these methods to sort through the timeline. we were able to find most of the logged activity, but were unable to find the specific websites visited using Google Chrome.

Further Work

There was not a significant amount of time allocated towards analysis due to time constraints, and so only a small amount of the logged activity was found. Further work could be done on this project to verify that log2timeline does extract all of the artifacts that it claims to support and to verify that all of the logged activity can be found. There also needs to be work to see if the inability to correctly parse Google Chrome history was a user error or a limitation of the tool, as the web activity generated by Chrome was not found. More work can also be done to see if the log2timeline-sift command will find the same artifacts as the individual log2timeline commands.

Table 1 - Activity Log

Date	Time	Action	Description
2/21/2013	15:04:30	Began install	Began Win7 enterprise 64 bit install
2/21/2013	15:15:45	Restart	Restart during install
2/21/2013	15:19:46	Restart	Restart during install
2/21/2013	15:21	Created User Name / Computer name	User Name: LCDI Computer Name: LCDI-PC
2/21/2013	3:22:30 PM	Set password	Passoword: forensics Hint: no
2/21/2013	3:23:45 PM	Windows update recommended settings and set timezone	Timezone: UTC -5 Eastern
2/21/2013	3:23:55 PM	Set network to home	Set network to home
2/21/2013	3:23:25 PM	Install finished	Install finsihed
2/21/2013	3:26:47 PM	Logged into desktop	At desktop
2/21/2013	3:27:06 PM	Opened Internet Explorer 8	Opened with MSN.com homepage
2/21/2013	3:27:10 PM	Windows update started in background	Bubble from notification area popped up
2/21/2013	3:28:12 PM	Declined IE start guide thing	It opened a windows.microsoft.com address telling me that my browser has been upgraded
2/21/2013	15:29:20	Google.com	then clicked install google chrome,
2/21/2013	3:30 PM	Clicked download chrome	Checked set as default browser, clicked accept
	15:30:45	Windows update finished and prompted to restart	
2/21/2013	15:31	Chrome install finsihed	Opened with a chrome sync sign in page and a chrome getting started page
2/21/2013	15:32:10	CNN.com	
2/21/2013	3:33:00 PM	Skype.com	
2/21/2013	15:33:20	downloads on skype.com	clicked get skype for windows desktop
2/21/2013	3:33:35 PM	started download	
2/21/2013	15:34:10	opened skypesetup.exe	choose english and to run when computer starts did not install skype click to call did not set bing or msn as homepage
2/21/2013	3:35:20 PM	Skype install finished	skype log in window opened
2/21/2013	15:35:50	restarted for windows update	
2/21/2013	3:39:25 PM	Logged into LCDI account	
2/21/2013	3:40:00 PM	Removed Win7 install disk	
2/21/2013	3:42:20 PM	Opened Chrome	
2/21/2013	3:42:25 PM	champlain.edu	
2/21/2013	3:43:30 PM	Inserted USB Flash drive	
2/21/2013	3:44:10 PM	twitter.com	
2/21/2013	3:44:35 PM	removed flash drive	
2/21/2013	3:45:05 PM	closed twitter.com	
2/21/2013	3:45:25 PM	created .txt on desktop	
2/21/2013	3:46:10 PM	renamed forenscs	
2/21/2013	3:47:00 PM	edited document	put in 'super secret stuff'
2/21/2013	3:47:15 PM	closed document	

2/21/2013	3:47:51 PM	opened chrome	
2/21/2013	3:48:20 PM	went to dropbox.com	
2/21/2013	3:48:40 PM	clicked download	new webpage, download started
2/21/2013	3:49:00 PM	opened dropbox installer	
2/21/2013	3:50:00 PM	install finished	dropbox opened
2/21/2013	3:50:45 PM	closed dropbox	
2/21/2013	15:52:35	closed dropbox website	
2/21/2013	3:54:07 PM	Shutdown computer	
2/21/2013	3:56:00 PM	Turned computer on	
2/21/2013	3:57:15 PM	logged in	dropbox and skype auto opened
2/21/2013	3:58:00 PM	closed dropbox	
2/21/2013	3:58:10 PM	closed skype	
2/21/2013	4:00:30 PM	opened chrome	
2/21/2013	4:01:00 PM	google gimp	
2/21/2013	4:01:20 PM	clicked gimp.org from google	
2/21/2013	4:01:50 PM	clicked download	
2/21/2013	4:02:15 PM	clicked download gimp 2.8.4	
2/21/2013	4:02:15 PM	brought to a sourceforge url where gimp auto downloaded	
2/21/2013	16:03	Opened gimp setup	ran install
2/21/2013	4:04:02 PM	install finished	
2/21/2013	16:04:25	closed chrome	
2/21/2013	4:05:30 PM	shut down computer	
2/28/2013	4:12:41 PM	turned on computer	
2/28/2013	4:14:00pm	logged in	
2/28/2013	4:19:00pm	exited dropbox	dropbox is set to auto login
2/28/2013	4:21:35pm	opened chrome	
2/28/2013	4:22:31PM	went to facebook.com	
2/28/2013	4:25:04pm	went to cnn.com	
2/28/2013	4:25:37pm	clicked one of the stories on cnn.com	"house passes violence against women act after GOP version defeated" was the article
2/28/2013	4:26:23pm	closed chrome	
2/28/2013	4:26:46pm	opened dropbox	
2/28/2013	4:27:07pm	opened dropbox preferences	
2/28/2013	4:27:27pm	turned off auto open for dropbox	
2/28/2013	4:27:48pm	closed dropbox	
2/28/2013	16:37:45	computer went to sleep	
2/28/2013	4:46:12pm	woke computer up	
2/28/2013	4:46:35pm	shut computer down	updates automatically installed

Table 2- Dell XPS Workstation

Windows 7 Enterprise SP1 64bit
Intel Core 2 Quad 2.66Ghz
6.00 GB RAM
NVIDIA GeForce 9800GT
Seagate Barracuda 250GB SATA HDD