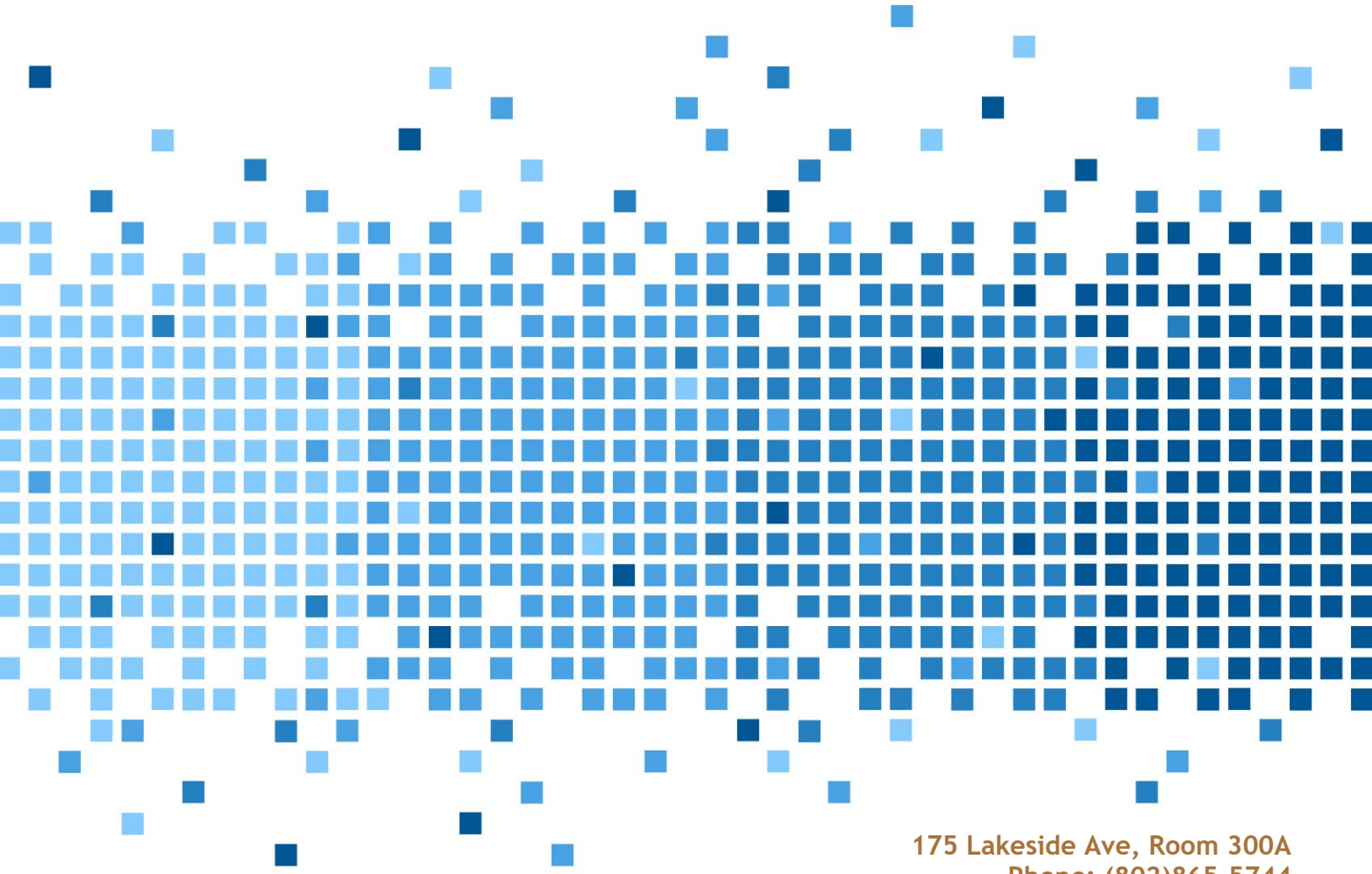
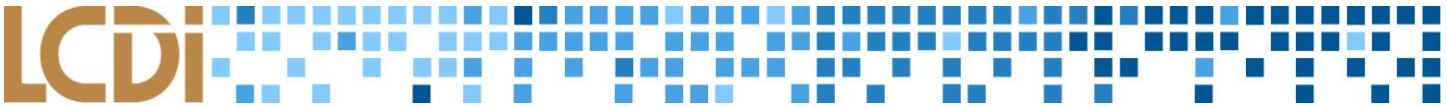
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

[Splunk Forensics]



175 Lakeside Ave, Room 300A
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

04/26/2016



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

Splunk is a cybersecurity tool widely used by network administrators, typically for real time data monitoring. For the purpose of our project, we wanted to determine if Splunk is a valid tool for temporal analysis in the realm of digital forensics. A forensic timeline is simply a timeline of events on a suspect machine. It has numerous uses for a digital forensic investigator ranging from temporal analysis to narrowing in on a specific time range for further investigation. Forensic timelines give the investigator a quick idea of when and what events happened on a particular system allowing them to narrow the scope of their investigation.

Many forensic tools offer timeline features both internally and with separate utilities. Some examples of software that can generate timelines include EnCase and Autopsy; however, these tools are not solely dedicated to the task, and usually fall short in results, speed, and usability. The main benefit to using these tools is that they are built into the forensic software and allow for further analysis of file data and content.

Background:

Splunk is primarily used to analyze large amounts of network data and provide timely reports useful to network administrators. A blog post from Klein & Co. discussed creating and analyzing a forensic timeline through the use of Splunk (Klein, 2011). We used this blog post as a starting point for our research. The blog outlines the step by step process of how to create a forensic timeline using command line tools and then explains how to upload and analyze the timeline using Splunk. This semester is the first time the LCDI has examined the option of using Splunk for digital forensics.

Purpose and Scope:

The purpose of this report is to serve as a resource for using Splunk as a forensic tool and to represent the effectiveness of Splunk in that capacity. The results of our research will be useful for investigators who are considering using Splunk to create a forensic timeline. Splunk is a commonly used program in the industry and may be able to assist investigators in future forensic investigations.

Research Questions:

Through our research into this project we developed a list of questions that we aimed to answer and make a determination on, including:

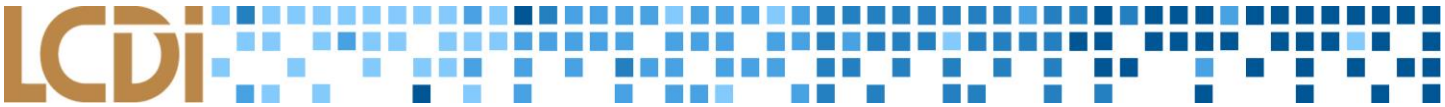
1. Is Splunk a valid forensic timelineing tool?
2. Is Splunk an effective forensic timelineing tool?
3. What can Splunk accurately tell us about the data?

Terminology:

Acquisition – The process of copying data from a piece of evidence to another location in a forensically sound manner so that the data may be analyzed at a later time. This is usually done by attaching some form of write blocking device to the storage media, and creating a copy of the data. The goal is to leave the original media intact while working on a copy of it. This allows for evidence to be verified at a later date. There are two different types of data acquisition methods: Physical and Logical.

Artifacts – Any data generated by user interaction that can be collected and examined. Any user data retrieved from the browser is considered an artifact, including cookies, caches, geolocation, search history, etc.

.Body Files – This file format is the default file format of commands fls and log2timeline. The general format of these files are data sets separated by a pipe "| ." The .body files are fed to the mactime command in order to create the .csv files that are needed for forensic timeline creation.



.CSV Files – CSV or comma separated value files are files where each piece of information, or value, is separated by a comma. CSV files can generally be read by spreadsheet programs, such as Microsoft Excel, where each new line is a row, and each column separator is a column.

File System – A file system is used to control how data is stored on a disk as well as retried off of a disk. Without a file system, the operating system would have no way of communicating directly with the disk. File systems store and organize the data on a disk in different ways. Different operating systems will use different file systems.

FTK Imager – A free extension of FTK 4.1. This is a powerful imaging program that can be used to create forensic images of a drive, which can then be opened in most forensic software for examination. There are other functions that allow this program to take images of specific files in a storage device as well as floppy disks, CDs, DVDs, and zip disks.

FLS (Command) – FLS is a command utility built into The Sleuth Kit and allows the user to extract timeline data from the filesystem. The -m argument will export the data into a body file which can then be converted using the mactime command.

HFS+ – HFS+, also known as Hierarchical File System Plus, is the default file system for Mac OSX. HFS+ is also utilized on Apple's portable devices and records metadata similarly to NTFS.

Image – A copy of a hard drive, or disk image, which is compressed into a series of files. Physical images include all information (zeroes and ones) on the hard drive whether the space is being used or not, and ends up being close to the same size as the actual hard drive itself. As opposed to a physical image, a logical image only acquires the parts of the hard drive that have active data and dismisses the rest of the drive. Compared to a physical image, the size can be extremely small or the same size as the drive depending on the amount of data stored.

Log2timeline (Command) – Log2timeline is a command utility that allows the examiner to create a timeline using artifacts and logs found on a system. Using the -o argument will export the data in the mactime format which can then be converted into a csv file.

MACB Times – MACB times refer to the timestamps on a file as they are given by the file system. MACB times correspond to Modified, Accessed, Created, and Birth respectively. Different File systems provide different timestamps and will change these timestamps in different ways.

Mactime (Command) – This command converts file in the .body file format to the useful .csv file format. This command comes stock with The Sleuth Kit.

NTFS – NTFS, also known as New Technology File System, is the default file system for Windows. NTFS supports metadata such as timestamps, improved performance, reliability, and more file extensions over older file systems. NTFS is one of the most common file systems seen today.

Operating System (OS) – A suite of programs that controls signals to and from input devices (such as a mouse, keyboard, microphone), peripherals (hard disks, CD/DVD drives, printers, etc.), output devices (monitors, speakers, etc.), and performs the basic functions needed for a computer to operate. This entails input and output, memory allocation, file management, task scheduling, etc. Having an OS is essential to operate a computer, as applications utilize the OS to function.

Sift Workstation – SIFT, also known as SANS Investigative Forensic Toolkit, is a forensics VMware appliance running off of Ubuntu Linux and comes preconfigured with all the required tools for a forensic examination. The workstation comes with the preinstalled tools Sleuth Kit and other commands such as log2timeline.

The Sleuth Kit – The Sleuth Kit is a set of forensic command line utilities. This utility has many useful commands built in such as the fls command and mactime. TSK is the command line version of Autopsy, the GUI supported version. The Sleuth Kit is compatible with many files systems ranging from NTFS to HFS+ to EXT4.

Splunk – Splunk is a data analytics tool that can quickly analyze vast amounts of data and represent those results in a distinguishable format such as a chart. Splunk is widely used throughout the cybersecurity and networking industry and has uses in the forensics field as well. Splunk accepts many types of data ranging from stagnant csv files to live network reports.

Virtual Machine (VM) – A virtual machine is a software-based computer that executes and runs programs like a physical machine. A virtual machine supports the execution of a complete operating system. VMs usually emulate an existing architecture and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use, or of having multiple instances of virtual machines.

.VMDK – The file extension denoting a VMs virtual hard drive.

Methodology and Methods

Overview:

For this project we chose to examine two different file systems: NTFS and HFS+. These two filesystems are the two most commonly used filesystem as they correspond to the two most commonly used operating systems. NTFS is the default file system for Windows and HFS+ is the default file system for Mac OS X.

Equipment Used:

Table 1: Software

Software	Version	Comments
VMware Fusion and VSphere		
Microsoft Windows 7	7	
Mac OS X	El Capitan	
Forensic Tool Kit Imager	3.4.2.2	
SANS Sift Workstation		Forensic workstation VM built by SANS. Comes prepacked with tools such as The Sleuth Kit.
Splunk Enterprise	6.4.0	Used Splunk free trial twice

Data Generation:

In order to start researching this project we had to conduct data generation on the two chosen operating systems. It was decided that it would be best to create a data generation script that we could use for both our Windows and Mac data generation cycles. We came up with a list of twenty items that we would perform for each OS:

1. Install OS
2. Create user account
3. Browse the web using the default browser
4. Install Google Chrome
5. Browse the web using Chrome

6. Install Firefox
7. Browse the web using Firefox
8. Download 5 images from Google
9. Install and use Office/Open Office
10. Create, modify, and delete multiple folders
11. Run commands in Command Line/Terminal
12. Install programs, then uninstall them
13. Change desktop background to a downloaded image
14. Create a second user account
15. Using OS default applications (calculator, snipping tool, print screen, etc.)
16. Take a screenshot and save it
17. Create sticky notes
18. Create text files, delete one
19. Open Paint and create images
20. Install and use Skype

For each action, we recorded the timestamp on the VM when the action was performed and comments about the action (i.e. files downloaded, deleted, renamed, etc.). We tried to record as much information as we could to make analysis easier.

Data Collection:

After generating data for both the Windows and Mac VMs, we used FTK Imager to virtually mount the VMDK files for each VM. Once they were mounted, we created a raw image (DD). This DD was then fed into our SIFT Workstation where we ran the following commands:

1. "fls –m "" –r image.dd > fls.body" [Extracts file system timestamps]
2. mactime –b fls.body –d > fls.csv [Corrects MACB data]
3. log2timeline -f exif,pdf,mft -o mactime –r -w log2timeline.body /mnt/volume [Pulls extra time data]
4. mactime –b log2timeline.body –d > log2timeline.csv [Corrects MACB data]

Running these commands created four different CSV files that we could then upload to Splunk. These CSV files contained the file system metadata only and did not contain any file content. We were then able to use Splunk to analyze the filesystem metadata and attempt to find evidence of our actions on the two different operating systems.

Analysis

Both the Mac and Windows timeline information presented very similar results. We expected to find more information from the Windows timeline than the Mac timeline purely due to NTFS cataloging most actions. What we found was that a lot of the data generation items could be found, provided one could access the data within certain locations (i.e. registry, internet database files, etc.). When comparing our data generation with the data on Splunk, we had to adjust for time differences. Our VMs were using EST/EDT (switched part way through this project) while Splunk was using UTC, resulting in a discrepancy of 4 or 5 hours off depending on which artifact we were looking at.

Results

Windows:

Despite being able to see only filesystem metadata, we were able to piece together a large portion of our data generation on Windows. For example, based on the creation timestamp for each user's NTUSER.DAT file, we could tell when the user first logged into the system. Below is a second user we created called Splunk2, with a created time on the NTUSER.DAT of 2/17/16 11:25:37 AM. This matched up to the time we recorded on our data generation sheet for when we logged into the account.

2/17/16 11:25:37.524 AM	/Users/Splunk2/NTUSER.DAT

We were also able to find various installation packages, LNK files, or installation executables for items we downloaded i.e. Skype, Chrome, Firefox, etc. These times matched up with our recorded data generation, though we were unable to piece together any actual activity created using these.

2/16/16 6:23:40.430 PM
Tue Feb 16 2016 18:23:40,43048960,.a.b,r/rrwxrwxrwx,0,0,215295-128-3,"/Users/Splunk/AppData/Local/Temp/Skype.msi"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/24/16 10:06:21.164 AM
Wed Feb 24 2016 10:06:21,164,.a.b,r/rrwxrwxrwx,0,0,61450-48-7,"/Users/Splunk/Downloads/Apache_OpenOffice_4.1.2_Win_x86_install_en-US.exe ($FILE_NAME)"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/23/16 8:55:15.968 AM
Tue Feb 23 2016 08:55:15,96823808,.a.b,r/rrwxrwxrwx,0,0,58267-128-10,"/Users/Splunk/Downloads/gimp-2.8.16-setup-1.exe"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/16/16 6:27:00.000 PM
Tue Feb 16 2016 18:27:00,0,macb,0,0,0,216633,"[EXIF metadata] (LNK/CreateDate) CreateDate (file: /Users/Public/Desktop/Mozilla Firefox.lnk)"
host = RESEARCH-11 | source = log2timeline.csv | sourcetype = csv

Along with downloaded applications, we were also able to find instances of our downloaded images. Surprisingly, we were also able to find both the downloaded image and what we renamed the image to. Below we have a Funny-Dog-Memes-Snake.lnk file, which is the downloaded image, and then below that we have a Dog Meme 2.lnk file, which is what we renamed the image to. This was consistent with every image we downloaded.

(LNK/AccessDate) AccessDate (file: /Users/Splunk/AppData/Roaming/Microsoft/Windows/Recent/Funny-Dog-Memes-Snake.lnk)"

(LNK/AccessDate) AccessDate (file: /Users/Splunk/AppData/Roaming/Microsoft/Windows/Recent/Dog Meme 2.lnk)"

Any document or image created on the machine was matched with the time of creation on our data generation sheet. We created folders, different documents, and took a screenshot using Microsoft's built-in Snipping Tool.

2/17/16 11:04:21.337 AM
Wed Feb 17 2016 11:04:21,337345,macb,r/rrwxrwxrwx,0,0,216040-128-3,"/Users/Splunk/Pictures/windows.PNG"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/24/16 10:28:25.117 AM
Wed Feb 24 2016 10:28:25,11790,..c.,r/rrwxrwxrwx,0,0,69698-128-4,"/Users/Splunk/Documents/Presentation.odp"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/24/16 10:26:22.110 AM
Wed Feb 24 2016 10:26:22,11081,..c.,r/rrwxrwxrwx,0,0,69670-128-4,"/Users/Splunk/Documents/Spreadsheet.ods"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/24/16 10:24:12.113 AM
Wed Feb 24 2016 10:24:12,11361,..c.,r/rrwxrwxrwx,0,0,69889-128-3,"/Users/Splunk/Documents/splunk.odt"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

2/16/16 6:20:37.125 PM
Tue Feb 16 2016 18:20:37,1252802,..c.,r/rrwxrwxrwx,0,0,214198-128-3,"/Users/Splunk/Documents/time.txt"
host = RESEARCH-11 | source = fls.csv | sourcetype = csv

*See Appendix 1 and Appendix 3 to see the full data generation sheet and Splunk results for Windows

Mac OS X:

While we only had access to filesystem metadata instead of full files, we were still able to locate a large portion of the artifacts that we created using OS X. We were able to identify certain operating system actions simply by looking at the MACB times of files and folders on the machine. For example, we were able to determine when a user was created by looking at their specific directory inside the user's directory. In this case we found that the second user's directory has a birth date of 3/2/2016 7:04:44PM which matches our data generation time.

_time	type	file
3/2/16 7:08:14.000 PM	m.c.	/Users/splunk2
3/2/16 7:04:44.000 PM	.a.b	/Users/splunk2

Splunk also gave us the ability to easily locate the MACB times of any file that was located on the system. Because of this it was easy for us to verify the times of any file that we created or placed on the machine. We created many folders, documents, and images on the virtual machine. As long as the file or directory was not later deleted and emptied from the trash we were able to find the evidence easily. For example, we took screen shots using the built in function on OS X and we were easily able to locate those files and match up the timestamps to the ones we marked in our data generation sheet.

_time	type	file
3/8/16 3:40:57.145 PM	macb	/Users/splunk/Desktop/Screen Shot 2016-03-08 at 10.40.53 AM.png
3/8/16 3:39:46.214 PM	macb	/Users/splunk/Desktop/Screen Shot 2016-03-08 at 10.39.41 AM.png
3/8/16 3:38:37.124 PM	...b	/Users/splunk/Desktop/Screen Shot 2016-03-08 at 10.38.37 AM.png

We were also able to detect when some programs were installed on the machine. By looking for files with the extension .dmg, the install file for OS X, we were able to determine when these files were last accessed and therefore used to install a program. One example of this is installing Skype. We located the install file for Skype and found that it had a last accessed time of 3/2/2016 8:07:35PM, which matched our note of when we installed the program in our data generation.

_time	type	file
3/2/16 8:07:36.442 PM	..c.	/Users/splunk/Downloads/Skype_7.21.350.dmg
3/2/16 8:07:35.442 PM	.a..	/Users/splunk/Downloads/Skype_7.21.350.dmg
3/2/16 8:07:15.442 PM	m...	/Users/splunk/Downloads/Skype_7.21.350.dmg
3/2/16 8:07:14.442 PM	...b	/Users/splunk/Downloads/Skype_7.21.350.dmg

While we were able to find a large portion of the artifacts that we created, some actions were not able to be located using only the filesystem metadata. The primary issue we had was that we couldn't find some data such as web browser history or the actual contents of the files we located. We also could not find items that were deleted and then removed from the trash. Once an item is removed from the trash it is no longer part of the filesystem records and as such was not extracted when we pulled the data. For example, we created a total of 6 directories in a folder on the desktop. We then deleted the second folder which contained folders 4 through 6. The trash was then emptied, and because of this, the only folders that have entries in Splunk are 1 through 3.

3/2/16 7:33:13.000 PM	m.c.	/Users/splunk/Desktop/NewDirectory/1
3/2/16 7:33:09.000 PM	macb	/Users/splunk/Desktop/NewDirectory/1/3
3/2/16 7:32:22.000 PM	.a.b	/Users/splunk/Desktop/NewDirectory/1

*See Appendix 2 and Appendix 4 for the full data generation sheet and full results for Mac

Conclusion

Is Splunk a valid forensic timelineing tool?

1. Splunk is a powerful tool for searching through logs and system data. However, finding data is completely determined by the user's ability to craft search terms. Due to this, data that you might expect to find easily is sometimes hidden by a faulty search term.
2. In addition, MACB times are separated by how they occur. For example, if the Modified and Created times are same there is one entry and then another entry is created for the Accessed time (if it exists). Should these times be separated, then the examiner has no way of knowing if the data is complete and valid.
3. Gaining access to the data is tricky. Numerous tools need to be used to get a valid csv to import into Splunk. Due to this, Splunk should only be used when the case or information set you need to search is large.

Is Splunk an effective forensic timelineing tool?

1. If you are only looking for MACB times of each file, yes. Splunk does not "dig deep"- it does not pull data from within the files, thus potentially missing important times. So if you are only looking when someone altered a file, Splunk performs well. Also, Splunk's timelineing ability does not show if the times displayed are UTC, EST, CST, etc. The examiner is expected to know this going in.
2. Due to the fact that Splunk does not provide the information that is inside files, it is best used with other forensics software such as FTK, Internet Evidence Finder, or EnCase.
3. Splunk is meant to be used in large enterprises where it processes terabytes of data, so the application as a whole is fast and responsive. Also, because of this, Splunk can easily be used for large scale network investigations with ease.

What can Splunk actually tell us about the data?

1. Splunk is dependent on its parent programs, namely fls, mactime, and log2timeline. Should these programs fail to find something, Splunk will not show this data. In addition, as previously said, Splunk can only access data it's given. In this case, it's MACB times and the file's location. In short, Splunk only gives data that it is fed, in our case MACB times and file locations.

Further Work

As with anything in forensics, further work can always be conducted and this project is no different. For this semester we only looked at two filesystems: NTFS and HFS+. While these are two of the most common file systems, many more are used and examiners will come into contact with them at times. The two main file systems that come to mind are FAT32 and EXT4. FAT32 is commonly used on flash drives and portable media devices. EXT4 is used inside of many Linux environments.

The process of extracting the timeline data, converting it to the .CSV format, and uploading it to Splunk is tedious. This process takes a large amount of time and requires a decent amount of expertise. This process could be automated through a simple script and would make using Splunk as a forensic tool a lot more viable. This process could be completed using various programming languages and would most likely run in a Linux environment.

Work could also be conducted into comparing and contrasting the differences between timelineing tools. Splunk is a very efficient and fast timelineing tool; however, you don't have access to the actual files while using Splunk. It would be beneficial to compare other forensic timelineing tools such as EnCase and Autopsy's tools to Splunk.

The final area of further work would be to examine other applications that operate similarly to Splunk. Splunk is an industry loved tool but for various reasons some investigators may not be able to access it. For this reason it would be beneficial to examine other applications with similar functionality.

Appendix

Appendix 1 Windows Data Gen:

Machine Timestamp	User Action	Comments
Time on VM		
2/16/2016 11:20:00	VM Created	
2/16/2016 11:36:00	Changed Time on Clock 3:36am > 11:36 am	
2/16/2016 11:40:00	Created 'Test Account'	Account name was changed to Splunk later in data gen so it appears as this username during analysis
2/16/2016 11:44:00	Created Password on 'Test Account' > Password	
2/16/2016 11:44:00	Created password hint for 'Test Account' > This is a password	
2/16/2016 11:47:00	Changed the picture for 'Test Account' from starfish to dog	
2/16/2016 11:48:00	Changed the picture for 'Splunk' from stairs to cat	
2/16/2016 11:50:00	Used IE to go to www.google.com	
2/16/2016 11:50:00	Searched for funny cat pictures	
2/16/2016 11:56:00	Downloaded two cat images	
2/16/2016 11:58:00	Used IE search bar (Bing) to search for "download google chrome"	
2/16/2016 12:01:00	Installed Google Chrome	
2/16/2016 12:12:00	Logged into mymail account	
2/16/2016 12:10:00	Used chrome to search for "funny dog memes"	
2/16/2016 12:18:00	Downloaded two dog memes	
2/16/2016 12:29:00	Downloaded another two dog memes	
2/16/2016 12:32:00	Went to www.youtube.com	
2/16/2016 12:33:00	Watched video "Mean Tweets - Music Edition #3"	
2/16/2016 12:52:00	Went to www.gmail.com	
2/16/2016 12:53:00	Sent an email from mymail to relytsw@gmail.com	
2/16/2016 12:53:00	Created a text document on desktop called "Random Text"	"This file is super cool because it contains random data that doesn't mean anything!"
2/16/2016 12:59:00	Sent an email from mymail to relytsw@gmail.com	Attached Random Text, 4-28-12-caturday....jpg, and Funny-Dog-Memes-Snake.jpg
2/16/2016 13:00:00	Renamed the downloaded images	dog-meme-20.jpg > Dog Meme 1, Funny-Dog.... > Dog Meme 2, funny-eyebrows > Dog Meme 3, Tumblr > Dog Meme 4, "poptart cat" > Cat Meme 1, "Meow Cat" > Cat Meme 2
2/16/2016 13:14:00	Went to www.yahoo.com	

Machine Timestamp	User Action	Comments
2/16/2016 13:15:00	Went to www.champlain.edu	
2/16/2016 13:16:00	Logged into Canvas	
2/16/2016 13:17:00	Went to drive.google.com	
2/16/2016 13:19:00	Downloaded "time.txt" from mymail google drive	
2/16/2016 13:20:00	Moved "time.txt" from Downloads > Documents	
2/16/2016 13:22:00	Went to www.google.com	
2/16/2016 13:23:00	Searched for Skype and downloaded/installed Skype	
2/16/2016 13:26:00	Searched for Firefox and downloaded/installed Firefox	
2/16/2016 13:33:00	Turned VM Off	
2/17/2016 5:29:00	Powered VM on	
2/17/2016 5:31:00	Logged into the Splunk account using the username and password	
2/17/2016 5:33:00	Time in VM reading 2/17/2016 5:33	
2/17/2016 5:35:00	opened Command Prompt from windows search bar	
2/17/2016 5:38:00	ran command "ping www.google.com"	Command didn't go through properly most likely because the internet is not connected
2/17/2016 5:39:00	closed command prompt	
2/17/2016 5:39:00	Opened paint and created an image	
2/17/2016 5:40:00	saved the image as "paint.png" to the desktop	
2/17/2016 5:41:00	Opened the image "paint.png" by double clicking on the image on the desktop	
2/17/2016 5:44:00	I added the picture "paint.png" to a compressed file and saved that as "paint.zip"	
2/17/2016 5:46:00	I deleted the picture "paint.png" from the desktop	
2/17/2016 5:48:00	I emptied the recycle bin	recycle bin contained only "paint.png"
2/17/2016 5:57:00	Set the machines background to "Dog Meme 2"	
2/17/2016 5:58:00	changed the desktop background back to the windows default	
2/17/2016 6:04:00	Used sniping tool to take an image of the windows logo on the desktop background. Saved that image as "windows.png" to the pictures directory	
2/17/2016 6:09:00	Created 3 sticky notes	Note 1: "This is sticky note one" Note 2: "How about #2" Note 3: "And finally 3"
2/17/2016 6:10:00	I deleted the third sticky note	
2/17/2016 6:18:00	I opened the calculator and ran a few operations through it, then closed it	(2+2), (10x79), and (565/5)
2/17/2016 6:22:00	Created a standard user account "Splunk 2" Added a password to it with a hint of "This is a password"	Username "splunk2" password "D@tagen!"
2/17/2016 6:24:00	changed Splunk2's picture to the sunflower	
2/17/2016 6:24:00	Logged out of Splunk account	
2/17/2016 6:25:00	Signed into Splunk2 and typed the password in incorrectly the first time	

Machine Timestamp	User Action	Comments
2/17/2016 6:28:00	Signed out of the Splunk2 account and signed back into the Splunk account	
2/17/2016 6:45:00	Created a few folders in the documents drive	All the below folders are nested in the documents folder Folder 1 -Folder 2 --Folder 4 ---Final Folder -Folder 3
2/17/2016 6:47:00	I deleted Folder 3 in the documents folder	I left the folder in the recycle bin for now at least
2/17/2016 6:48:00	Machine got disconnected because the server was reset while I was using it.	The ESXI server was reset by Alex and I lost connection to the machine.
2/23/2016 2:07:00	Powered on Virtual Machine	
2/23/2016 2:08:00	Signed into Splunk account	Windows said that it did not have a valid activation key
2/23/2016 2:11:00	Opened Google Chrome	
2/23/2016 2:12:00	I navigated to www.google.com	
2/23/2016 2:18:00	I closed google chrome	
2/23/2016 2:19:00	I opened Firefox searched for an article about the apple san Bernardino incident	Went to the following sites- www.google.com - searched "apple san Bernardino" Went to NBC News site and read an article titled "Bill Gates Backs FBI....."
2/23/2016 2:24:00	I went to Wikipedia and clicked through 5 random articles	The articles were- The Cell Psychological thriller thriller Film genre Film theory
2/23/2016 2:27:00	Closed Firefox	
2/23/2016 3:02:00	I shutdown the VM	
2/23/2016 3:48:00	Started Up VM	
2/23/2016 3:50:00	Took a screenshot and saved it.	
2/23/2016 3:55:00	Downloaded Gimp via Chrome	
2/23/2016 3:56:00	Installed Gimp	
2/23/2016 3:59:00	Ran Gimp	
2/23/2016 4:02:00	Uninstalled Gimp	

Machine Timestamp	User Action	Comments
2/23/2016 4:05:00	Emptied Recycle Bin	
2/23/2016 4:10:00	Downloaded Python 3.5.1	
2/23/2016 4:13:00	Installed Python 3.5.1	Placed python onto the PATH as well.
2/23/2016 4:17:00	Started python interpreter via CMD	
2/23/2016 4:18:00	Ran several python commands	import math, return the value of math.pi, import os, played inside of os
2/23/2016 4:32:00	Uninstalled Python 3.5.1	
2/23/2016 4:35:00	Uninstalled Python 3.5.1 Launcher	
2/23/2016 4:37:00	Started download of OpenOffice	
2/23/2016 4:49:00	VM shutdown for some reason	
2/23/2016 5:04:00	Restarted VMware, download for open office is useless. I Deleted it.	Bad Download Name: Unconfirmed 129834.crdownload
2/23/2016 5:07:00	Emptied recycle Bin	
2/23/2016 5:09:00	Shutdown VM	
2/23/2016 17:35:00	Turned VM on	
2/23/2016 17:35:00	Adjusted clock on VM to match actual machine	
2/23/2016 12:42:00	Locked computer	
2/24/2016 5:02:00	Powered On the machine	
2/24/2016 5:02:00	Logged into the Splunk account	
2/24/2016 5:03:00	Created a new text document called "Text Doc" in the documents folder and added text	Added the text "This is probably the last text document I will add to this machine"
2/24/2016 5:05:00	Opened Chrome and started to download open office	The download took a while
2/24/2016 5:17:00	Installed open office	I set the username as "Splunk" I did a typical install and added a desktop shortcut
2/24/2016 5:22:00	Opened open office writer and created a document	
2/24/2016 5:24:00	Saved the document as "splunk.odt" to the documents folder	
2/24/2016 5:25:00	Opened Open office Calc and created a document with some random information	
2/24/2016 5:26:00	Saved the calc document as "Spreadsheet.ods" in the documents folder	
2/24/2016 5:26:00	Opened open office impress and created a presentation	
2/24/2016 5:28:00	Saved the presentation as "Presentation.odp" in the documents folder	
2/24/2016 5:28:00	I shutdown the machine	

Appendix 2 Mac Data Gen:

Machine Timestamp	User Action	Comments
3/1/201611:39	Started VM Install	
3/2/2016 12:57:00	Created an account	Name- Splunk Forensics Username- Splunk Password- In Secret Server Hint- "See Secret Server"
3/2/2016 13:00:00	Set Time zone to EST With closets city being NY City	
3/2/2016 13:10:00	Shutdown the VM	
3/2/2016 13:18:00	Started up the VM	
3/2/2016 13:24:00	Changed the "Splunk" account picture	Changed it to the default image of the fortune cookie.
3/2/2016 13:27:00	Used Safari to go to google (www.google.com)	
3/2/2016 13:27:00	Searched for "funny cat pictures"	Downloaded two images. Saved the first one as "pew pew pew" and the second as the default name
3/2/2016 13:31:00	Installed Google Chrome	Clicked on the link in google to download google chrome and then installed it
3/2/2016 13:33:00	Opened google chrome	Did not set as default browser
3/2/2016 13:35:00	Installed Firefox using google chrome	
3/2/2016 13:41:00	Downloaded open office	Downloaded using google chrome
3/2/2016 13:56:00	Installed Open Office Once it finished downloading	
3/2/2016 14:01:00	Restarted the VM	
3/2/2016 14:04:00	Created a second user account	Standard account, username- "splunk2" password is the same as Splunk account
3/2/2016 14:05:00	Signed out of the Splunk account	
3/2/2016 14:05:00	Signed into the splunk2 account	Did not link a iCloud account
3/2/2016 14:07:00	Changed splunk2 account image to the eagle default image	
3/2/2016 14:08:00	Signed out of splunk2 account	
3/2/2016 14:12:00	Signed into Splunk account	
3/2/2016 14:13:00	Opened terminal and ran a few commands	ran ifconfig, ping www.google.com, cd to desktop, mkdir NewDirectory
3/2/0216 14:20:00	Opened chrome and downloaded 5 images	Saved 3 to desktop and

Machine Timestamp	User Action	Comments
		2 to documents folder
3/2/2016 14:22:00	Changed the desktop background to one of the downloaded images	Changed it to the first downloaded image "path.jpg"
3/2/2016 14:23:00	Moved images from the desktop to the trash	
3/2/2016 14:32:00	Create folder in the NewDirectory folder on the desktop as follows	NewDirectory -1 --3 -2 --4 --5 ---6
3/2/2016 14:35:00	Deleted folder 2 and therefore all the folders underneath it	
3/2/2016 14:38:00	Emptied the recycle bin	
3/2/2016 14:55:00	Create 3 sticky notes and then closed one of them	
3/2/2016 15:06:00	Opened chrome and downloaded skype	
3/2/2016 15:07:00	Installed skype	Installed but did not use skype
3/2/2016 15:25:00	Shutdown the VM	
3/8/2016 9:28:00	Powered on Virtual Machine	
3/8/2016 9:30:00	Singed into the Splunk Forensics account	
3/8/2016 9:37:00	Opened then closed safari	
3/8/2016 9:40:00	Opened Firefox	Didn't import data from any other browsers Went to Wikipedia and opened a random article then clicked the first linked item on the page, did this five times Went to www.champlain.edu and navigated around
3/8/2016 9:50:00	Closed Firefox	
3/8/2016 9:54:00	Opened Open Office and set it up	First Name - Splunk Last Name - Forensics Initial - S
3/8/2016 10:02:00	Created a text document and saved it	Saved it as "Text_1" in the documents folder
3/8/2016 10:05:00	Created a spreadsheet and saved it	Saved it as "Spreadsheet_1" in the documents folder
3/8/2016 10:08:00	Created a presentation and saved it	Saved it as (Presentation) on the Desktop
3/8/2016 10:11:00	Closed Open Office	
3/8/2016 10:11:00	Put the machine to sleep	
3/8/2016 10:17:00	Opened Chrome and downloaded Gimp	

Machine Timestamp	User Action	Comments
3/8/2016 10:20:00	Opened Gimp	
3/8/2016 10:27:00	Closed Gimp	
3/8/2016 10:28:00	Uninstalled Gimp	
3/8/2016 10:30:00	Opened Safari and downloaded python 3.5.1	
3/8/2016 10:31:00	Installed Python	
3/8/2016 10:32:00	Opened Python	
3/8/2016 10:35:00	Uninstalled Python	
3/8/2016 10:36:00	Emptied the trash	
3/8/2016 10:38:00	Took a screenshot	Equivalent to print screen on windows, it saved automatically to the desktop
3/8/2016 10:39:00	Used the mac Snipping tool to take a picture of part of the desktop	
3/8/2016 10:40:00	Took a screenshot of the finder window	
3/8/2016 10:41:00	Opened Text Edit and create two docs	Desktop_Text saved to desktop Documents_Text saved to desktop
3/8/2016 10:45:00	Opened preview and edited a picture using the paint features in preview	Opened the screenshot and scribbled on it
3/8/2016 10:47:00	Shutdown the VM	

Appendix 3 Windows Results:

Machine Timestamp	User Action	Evidence Found
2/16/2016 11:20:00	VM Created	
2/16/2016 11:36:00	Changed Time on Clock 3:36am > 11:36 am	
2/16/2016 11:40:00	Created 'Test Account'	Found Both the users directory and the NTUSER.DAT with a created time of 7:58:15, this doesn't match up with the time recorded but is when the account was supposed to be created
2/16/2016 11:44:00	Created Password on 'Test Account' > Password	Not Found
2/16/2016 11:44:00	Created password hint for 'Test Account' > This is a password	Not Found
2/16/2016 11:47:00	Changed the picture for 'Test Account' from starfish to dog	Not Found
2/16/2016 11:48:00	Changed the picture for 'Splunk' from stairs to cat	Not Found
2/16/2016 11:50:00	Used IE to go to www.google.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 11:50:00	Searched for funny cat pictures	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 11:56:00	Downloaded two cat images	Foun the files with matching timestmaps
2/16/2016 11:58:00	Used IE search bar (bing) to search for "download google chrome"	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 12:01:00	Installed Google Chrome	Found the installer package with a last accessed time mathcing the recorded time
2/16/2016 12:12:00	Logged into mymail account	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 12:10:00	Used chrome to search for "funny dog memes"	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 12:18:00	Downloaded two dog memes	Found the files with matchign timestmaps
2/16/2016 12:29:00	Downloaded another two dog memes	Found the files with matchign timestmaps
2/16/2016 12:32:00	Went to www.youtube.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 12:33:00	Watched video "Mean Tweets - Music Edition #3"	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata

Machine Timestamp	User Action	Evidence Found
2/16/2016 12:52:00	Went to www.gmail.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 12:53:00	Sent an email from mymail to relytsw@gmail.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 12:53:00	Created a text document on desktop called "Random Text"	Found the file, but not the text since that goes beyond metadata
2/16/2016 12:59:00	Sent an email from mymail to relytsw@gmail.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 13:00:00	Renamed the downloaded images	Nothing that says the images were renamed, but you can find evidence of both the original images and the renamed ones
2/16/2016 13:14:00	Went to www.yahoo.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 13:15:00	Went to www.champlain.edu	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 13:16:00	Logged into Canvas	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 13:17:00	Went to drive.google.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 13:19:00	Downloaded "time.txt" from mymail google drive	Evidence of this can't be found because it no longer exists in this location
2/16/2016 13:20:00	Moved "time.txt" from Downloads > Documents	Found the document in the new location, but not that it was actually moved
2/16/2016 13:22:00	Went to www.google.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/16/2016 13:23:00	Searched for Skype and downloaded/installed Skype	Found Installation Package
2/16/2016 13:26:00	Searched for Firefox and downloaded/installed Firefox	Found Installation Package
2/16/2016 13:33:00	Turned VM Off	All normal machine actions end after 6:33
2/17/2016 5:29:00	Powered VM on	Machine actions start again at 10:30 am
2/17/2016 5:31:00	Logged into the splunk account using the username and password	Would require data sources outside of what we gave splunk
2/17/2016 5:33:00	Time in VM reading 2/17/2016 5:33	Time matches

Machine Timestamp	User Action	Evidence Found
2/17/2016 5:35:00	opened Command Prompt from windows search bar	Searched for cmd.exe and could not find an events on this data
2/17/2016 5:38:00	ran comand "ping www.google.com"	can only find evidence that command prompt was opened but not what commands were used
2/17/2016 5:39:00	closed command prompt	Searched for cmd.exe and could not find an events on this date
2/17/2016 5:39:00	Opened paint and created an image	Searched for mspaint.exe and could not find any events on this date
2/17/2016 5:40:00	saved the image as "paint.png" to the desktop	Can't be found because it was emptied from the recycle bin and therefore did not have an entry in the MFT
2/17/2016 5:41:00	Opened the image "paint.png" by double clicking on the image on the desktop	Can't be found because it was emptied from the recycle bin and therefore did not have an entry in the MFT
2/17/2016 5:44:00	I added the picture "paint.png" to a compressed file and saved that as "paint.zip"	Found the file with a macb time of 10:45:00 which matches the timestamp
2/17/2016 5:46:00	I deleted the picture "paint.png" from the desktop	Can't be found because it was emptied from the recycle bin and therefore did not have an entry in the MFT
2/17/2016 5:48:00	I emptied the recycle bin	Can't find using only file system metadata
2/17/2016 5:57:00	Set the machines background to "Dog Meme 2"	Not found
2/17/2016 5:58:00	changed the desktop background back to the windows default	Not found
2/17/2016 6:04:00	Used sniping tool to take an image of the windows logo on the desktop background. Saved that image as "windows.png" to the pictures directory	Found the file
2/17/2016 6:09:00	Created 3 sticky notes	Found the StickyNotes.snt file with a birth time of 11:09:07 but can't tell what specific notes were created without having the actual file
2/17/2016 6:10:00	I deleted the third sticky note	Can only tell that the sticky note file was accessed not details on a specific sticky note
2/17/2016 6:18:00	I opened the calculator and ran a few operations through it, then closed it	Windows doesn't store calculator artifacts from what I can tell
2/17/2016 6:22:00	Created a standard user account "Splunk 2" Added a password to it with a hint of "This is a password"	User data is not created until first logon and the login details are stored in the registry which can't be viewed by splunk with the files we provided
2/17/2016 6:24:00	changed Splunk2's picture to the sunflower	Not found
2/17/2016 6:24:00	Logged out of Splunk account	Not found
2/17/2016 6:25:00	Signed into Splunk2 and typed the password in incorrectly the first time	Found the NTUSER.DAT for splunk2 with a birth time of 2/17/16 11:25:37.250 AM and this indicates the first logon of this user. NTUSER is always created the first time a user logs on

Machine Timestamp	User Action	Evidence Found
2/17/2016 6:28:00	Signed out of the Splunk2 account and signed back into the splunk account	The NTUSER.DAT for splunk2 was last modified on 2/17/16 11:28:37 and this is one of the last things changed on log off
2/17/2016 6:45:00	Created a few folders in the documents drive	Folder 3 was not present in documents
2/17/2016 6:47:00	I deleted Folder 3 in the documents folder	Because the recycle bin was later emptied this file is not listed
2/17/2016 6:48:00	Machine got disconnected because the server was reset while I was using it.	Machine activity ends abruptly
2/23/2016 2:07:00	Powered on Virtual Machine	Normal machine activity starts back up at this time
2/23/2016 2:08:00	Signed into splunk account	Can't tell when a user logs on just by using file system metadata
2/23/2016 2:11:00	Opened Google Chrome	Would require more information than just filesystem metadata
2/23/2016 2:12:00	I navigated to www.google.com	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/23/2016 2:18:00	I closed google chrome	Would require more information than just filesystem metadata
2/23/2016 2:19:00	I opened firefox searched for an article about the apple san bernardino incident	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/23/2016 2:24:00	I went to wikipedia and clicked through 5 random articles	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata
2/23/2016 2:27:00	Closed Firefox	Would require more information than just filesystem metadata
2/23/2016 3:02:00	I shutdown the VM	All user actions stop at this time, some exif data is spread out but machine data stops
2/23/2016 3:48:00	Started Up VM	Entries start again at this time
2/23/2016 3:50:00	Took a screenshot and saved it.	Found the screenshot with matchign tiemstamps
2/23/2016 3:55:00	Downloaded Gimp via Chrome	Found the file in downloads directroy with a created date of the download time
2/23/2016 3:56:00	Installed Gimp	Found the gimp setup exe and it has a accessed time of 2/23/16 8:55:15.968 AM and many of the gimp files have similar created or birth times
2/23/2016 3:59:00	Ran Gimp	Because the files are removed we were unable to locate them
2/23/2016 4:02:00	Uninstalled Gimp	Because the files are removed we were unable to locate them
2/23/2016 4:05:00	Emptied Recycle Bin	Can't be found because files are removed from recycle bin
2/23/2016 4:10:00	Downloaded Python 3.5.1	File was removed from the downloads directory so we were unable to locate it

Machine Timestamp	User Action	Evidence Found
2/23/2016 4:13:00	Installed Python 3.5.1	Found isntaller package with an accessed time that matches install time
2/23/2016 4:17:00	Started python interpreter via CMD	Because the files are removed we were unable to locate them
2/23/2016 4:18:00	Ran several python commands	Filesystem metadata can't tell us specifics on the commands run
2/23/2016 4:32:00	Uninstalled Python 3.5.1	Because the files are removed we were unable to locate them
2/23/2016 4:35:00	Uninstalled Python 3.5.1 Launcher	Because the files are removed we were unable to locate them
2/23/2016 4:37:00	Started download of OpenOffice	Because the files are removed we were unable to locate them
2/23/2016 4:49:00	VM shutdown for some reason	Computer activity stops at this time
2/23/2016 5:04:00	Restarted VMware, download for openoffice is useless.i Deleted it.	Because the recycle bin was emptied no filesystem metadata exists
2/23/2016 5:07:00	Emptied recycle Bin	Can't be found because files are removed from recycle bin
2/23/2016 5:09:00	Shutdown VM	Can find a break in any activity on the machine starting at 10:09, this indicates that the machine was shut off because nothing occurred.
2/23/2016 17:35:00	Turned VM on	Machine files start aperaing again at this time
2/23/2016 17:35:00	Adjusted clock on VM to match actual machine	Timestamps match but can't find this action specifically
2/23/2016 12:42:00	Locked computer	Would require data sources other than file system metadata to determine this
2/24/2016 5:02:00	Powered On the machine	Machine files start aperaing again at this time
2/24/2016 5:02:00	Logged into the splunk account	Can't be found
2/24/2016 5:03:00	Created a new text document called "Text Doc" in the documents folder and added text	Found the file with a created date of 2/24/16 10:04:33.670 time is a little off but the error may come from data gen records not timestamp
2/24/2016 5:05:00	Opened Chrome and started to download open office	Found the installer .exe file with a created date of 2/24/16 10:17:20.260. When files are downloaded their created date becomes the time they were downloaded.
2/24/2016 5:17:00	Installed openoffice	AM vs PM issue
2/24/2016 5:22:00	Opened open office writer and created a document	Can see a lot of activity for this application around this time but not sure if it proves activity or not
2/24/2016 5:24:00	Saved the document as "splunk.odt" to the documents folder	time matches up, though Splunk is displaying 10:24 AM instead of PM
2/24/2016 5:25:00	Opened Openoffice calc and created a document with some random information	Can see a lot of activity for this application around this time but not sure if it proves activity or not
2/24/2016 5:26:00	Saved the calc document as "Spreadsheet.ods" in the documents folder	time matches up, though Splunk is displaying 10:26 AM instead of PM

Machine Timestamp	User Action	Evidence Found
2/24/2016 5:26:00	Opened openoffice impress and created a presentation	Can see a lot of activity for this application around this time but not sure if it proves activity or not
2/24/2016 5:28:00	Saved the presentation as "Presentation.odp" in the documents folder	time matches up, though Splunk is displaying 10:28 AM instead of PM
2/24/2016 5:28:00	I shutdown the machine	All normal user activity ends after 10:28:00 the only entries after this are exif metadata

Appendix 4 Mac Results:

Machine Timestamp	User Action	Evidence Found
3/1/2016 11:39	Started VM Install	
3/2/2016 12:57:00	Created an account	Users/splunk directory created 3/2/16 6:01:20 PM, found the plist for the password hash for the account
3/2/2016 13:00:00	Set Timezone to EST With closets city beign NY City	/Library/Preferences/.GlobalPreferences.plist is where the timezone info should be located; however, wasn't able to find this file nor would you be able to see into it anyway
3/2/2016 13:10:00	Shutdown the VM	Possibly found in /private/var/db/systemstats/*, but hard to confirm what the files actually mean. Some correlate with the datagen times, while others don't
3/2/2016 13:18:00	Started up the VM	Possibly found in /private/var/db/systemstats/*, but hard to confirm what the files actually mean. Some correlate with the datagen times, while others don't
3/2/2016 13:24:00	Changed the "splunk" account picture	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata. You can, however, see a .db file created at the time of datagen browsing
3/2/2016 13:27:00	Used Safari to go to google (www.google.com)	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata. You can, however, see a .db file created at the time of datagen browsing
3/2/2016 13:27:00	Searched for "funny cat pictures"	Web history items can't be directly found in Splunk, this would require looking at specific files, splunk only has access to file system metadata. You can, however, see a .db file created at the time of datagen browsing
3/2/2016 13:31:00	Installed Google Chrome	Found the .dmg file with an accessed date of 3/2/16 6:32:29.661 PM
3/2/2016 13:33:00	Opened google chrome	Can see a lot of activity in the chrome directories but haven't found actual application yet
3/2/2016 13:35:00	Installed firefox using google chrome	Found the .dmg file with an accessed date of 3/2/16 6:36:45.824 PM
3/2/2016 13:41:00	Downloaded open office	Found the .dmg file with a birth time of 3/2/16 6:41:09.172 This indicates the time the downloaded started
3/2/2016 13:56:00	Installed Open Office Once it finished downloading	Found the .dmg file with an accessed date of 3/2/16 6:56:09.172 PM

Machine Timestamp	User Action	Evidence Found
3/2/2016 14:01:00	Restarted the VM	VM activity stops for a minute or two at this time
3/2/2016 14:04:00	Created a second user account	Found the users directory with a birth date of 3/2/16 7:04:44.000 PM
3/2/2016 14:05:00	Signed out of the splunk account	Would require additoinal information that was not given to splnk
3/2/2016 14:05:00	Signed into the splunk2 account	The created time for this users directory matches the last logoff not the first login which is odd
3/2/2016 14:07:00	Changed splunk2 account image to the eagle default image	Can see that the picture was changed but not what image it is or was
3/2/2016 14:08:00	Signed out of splunk2 account	The users directory was last modified at this time
3/2/2016 14:12:00	Signed into splunk account	Not found
3/2/2016 14:13:00	Opened terminal and ran a few commands	Found the Mac terminal folder which has an accessed time of 3/2/16 7:13:36.105 PM. The directory is "/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal" Unable to tell which commands were run
3/2/0216 14:20:00	Opened chrome and downloaded 5 images	Found a Funny-Cat-...-49.jpg and 2 pew pew pew.jpg in /Users/splunk/Downloads
3/2/2016 14:22:00	Changed the desktop background to one of the downloaded images	Not found
3/2/2016 14:23:00	Moved images from the desktop to the trash	Because it was deleted no file system metadata exists
3/2/2016 14:32:00	Create folder in the NewDirectory folder on the desktop as follows	Found directories 1 and 3 but was not able to locate any others because they were delted and removed from the trash
3/2/2016 14:35:00	Deleted folder 2 and therefore all the folders underneath it	Because the trash was empited no filesystem metadata exists
3/2/2016 14:38:00	Emptied the recycle bin	Because the trash was empited no filesystem metadata exists
3/2/2016 14:55:00	Create 3 sticky notes and then closed one of them	*/Library/StickiesDatabase contains stickies. Though we can't see what stickies there are, the created time matches that on the data gen
3/2/2016 15:06:00	Opened chrome and downloaded skype	Found the .dmg file with a birth time of 3/2/16 8:07:14.442 PM
3/2/2016 15:07:00	Installed skype	Found the .dmg file with an accessed time of 3/2/16 8:07:35.442 PM
3/2/2016 15:25:00	Shutdown the VM	All machine action ends at this point
3/8/2016 9:28:00	Powered on Virtual Machine	Machien actions start again
3/8/2016 9:30:00	Singed into the Splunk Forensics account	Not Found
3/8/2016 9:37:00	Opened then closed safari	Found Safari artifacts correlating to the time on the datagen sheet under /Users/splunk/Library/Safari
3/8/2016 9:40:00	Opened Firefox	For some reason could not find evdience

Machine Timestamp	User Action	Evidence Found
3/8/2016 9:50:00	Closed Firefox	For some reason could not find evdience
3/8/2016 9:54:00	Opened Open Office and set it up	Found Actual .app for running the program as well as bootcache
3/8/2016 10:02:00	Created a text document and saved it	Found Openoffice document with a created time of 3/8/16 3:02:09.166 PM
3/8/2016 10:05:00	Created a spreadsheet and saved it	Found openoffice spreadsheet with a macb time of 3/8/16 3:05:10.123 PM
3/8/2016 10:08:00	Created a presentation and saved it	Found Openoffice presentation with a created time of 3/8/16 3:08:48:141 PM
3/8/2016 10:11:00	Closed Open Office	Last accessed of this profam is at this time
3/8/2016 10:11:00	Put the machine to sleep	Found Sleep directory accessed at 3/8/2106
3/8/2016 10:17:00	Opened Chrome and downloaded Gimp	Found GIMP artifacts appearing around the time it was installed, but no direct download file found so far
3/8/2016 10:20:00	Opened Gimp	Not found because it was deleted
3/8/2016 10:27:00	Closed Gimp	Not found because it was deleted
3/8/2016 10:28:00	Uninstalled Gimp	Not found because it was deleted
3/8/2016 10:30:00	Opened Safari and downloaded python 3.5.1	Found the python package in the /Users/splunk/Downloads folder
3/8/2016 10:31:00	Installed Python	Found a PLIST/InstallDate for python
3/8/2016 10:32:00	Opened Python	Becaus the applcaiton was deleted it does not exist in filesystem metadata
3/8/2016 10:35:00	Uninstalled Python	While the main applicatoin file is gone I was still able to locate multipl epython files on the machine
3/8/2016 10:36:00	Emptied the trash	Not Found
3/8/2016 10:38:00	Took a screenshot	Found this file with mac time of 3/8/16 3:46:34.124 PM
3/8/2016 10:39:00	Used the mac Snipping tool to take a picture of part of the desktop	Found this file with macb time of 3/8/16 3:39:46.214 PM
3/8/2016 10:40:00	Took a screenshot of the finder window	Found this file with macb time of 3/8/16 3:40:57.145 PM
3/8/2016 10:41:00	Opened Text Edit and create two docs	Found Desktop_Text with a created time of 3/8/16 3:43:53.378 PM Found Documents_Text with a macb time of 3/8/16 3:44:43:398 PM
3/8/2016 10:45:00	Opened preview and edited a picture using the paint features in preview	Can see the last modifed date for this file and it matches the time recorded
3/8/2016 10:47:00	Shutdown the VM	If you look at the timeline for this day you can see that all activity ends after the time block for 3:47. Further investigation shows an event created under /private/var/db/systemstats/ which is responsible for maintaining a "snapshot" of the machine

References

Klein, N. (2011, November 19). Forensic timeline Splunking. Retrieved April 21, 2016