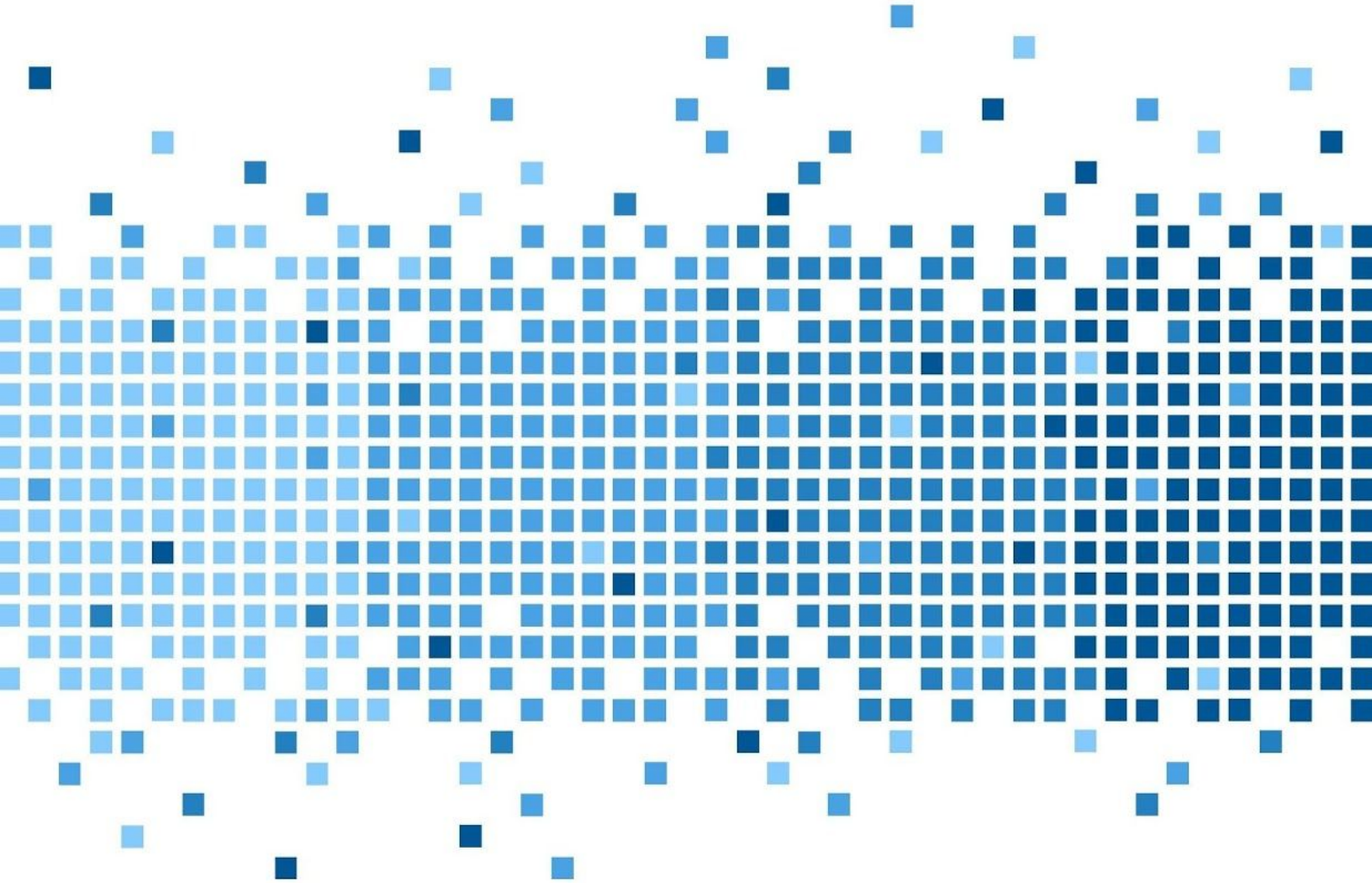
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

VMware Analysis



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

The ever-increasing interest in virtualization technology means that it's becoming more important for forensic investigators to understand how virtual machines can be analyzed in comparison to physical machines. Virtual machines (VMs) make it easy for users to work with multiple operating systems on a single computer. They create a digital environment in which all of the functions of a physical computer and operating system are simulated and can be used within the VM software without influencing the physical machine on which it is being used. In this project, the LCDI team is looking for differences in artifact discovery between virtual machines and physical machines.

Background

This project is drawn from many research projects previously conducted by the LCDI. These projects include: Windows 8 Forensics, Windows 10 forensics, and Jump List Forensics. The Windows 10 and Windows 8 Forensic projects focused on forensic artifacts that were updated, new, and/or similar between Windows 7, 8, and 10, including:

- Event Logs
- Internet Explorer
- USB Activity
- LNK Files
- Recycle Bin
- Thumbnails
- OneDrive
- Prefetch Files

The Jump List project focused on looking for relevant forensic artifacts. The Jump List, a taskbar feature, was first included in Windows 7 and has since been included in 8 and 10. The main focus of the Jump List project was to determine if the Jump List could be used to establish an effective timeline in forensic cases.

This current project not only reviews the facts established in the previous reports, but also covers some of the areas in which those reports needed further work. The differences of forensic artifacts between the OS's have been well documented. The research that was conducted in examination of the differences between VMs and physical machines has found that, "an imaged/mounted virtual machine is nearly identical, if not completely identical, to that of an imaged physical computer system or actual media" (Shavers, 2008). The referenced article goes on to explain that the only differences between the two would be that for a VM, "the system metadata associated with the virtual files and the virtual application as they reside on the host machine may give additional information that may be of importance" (Shavers, 2008).

Purpose and Scope

The purpose of this research project is to take a Windows operating system and install it onto a physical machine and a virtual machine. We want to see if there are any differences between the physical machine and VM in terms of file locations. The results of this project will be useful for future investigations, as the implementation of VMs are becoming more and more common. They are becoming more cost effective to implement, and allow for a sandbox environment that is easy and quick to set up.

Research Questions

1. What artifact locations are different between a physical machine and a VM, both running Windows 7?
2. What artifact locations are different between a physical machine and a VM, both running Windows 10?
3. What are the differences between the artifact findings from Windows 7 and Windows 10?

Terminology

Encase V7 - A suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use.

Forensics Image - An image often refers to a copy of a hard drive, or disk image, that 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. 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.

Forensic Toolkit (FTK) - A forensic tool made by AccessData. FTK allows users to acquire, process, and verify evidence. FTK supports many image formats. The current model is Version 5.6. Version 4.1 may also be used in our lab.

FTK Imager - This imager is 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.

LNK Files - LNK files are Windows shortcut files that you see on the Desktop and in various folders. LNK files provide the following about the original/target file: location (full path where the file is stored), filename, size of target file, target timestamps (created, accessed, modified), and file attributes (read only, system, hidden). It can also tell you information of the original volume the file is stored on such as: storage media type (fixed disk, CD, removable media), volume serial number, machine MAC address, and birth/current volume ID.

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.

Prefetch Files - Prefetch files are files with the extension .pf located in the C:/Windows/Prefetch directory. The files are created on a Windows machine when an application is run from a particular location for the first time. This is used to help speed up the loading of applications. These files contain: the file path for files/folders accessed during the first 10 seconds of application run, number of times application was run, last time application was run, and media information for volumes accessed (volume serial number, volume creation date).

RAM - An integrated circuit into which data can be read or written by a microprocessor or other device. The memory is volatile and will be lost if the system is disconnected from its power source.

SIFT(SANS Investigative Forensic Toolkit) - A computer forensics VMware appliance that comes preconfigured with all the required tools for a forensic examination.

Virtual Machine - 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. This leads to more efficient use of computing resources, both in terms of energy consumption and cost effectiveness (known as hardware virtualization, the key to a cloud computing environment).

VMware Tools - VMware Tools improves the performance and management of the virtual machine. VMware Tools is a suite of utilities that is installed in the operating system of a virtual machine. VMware Tools enhances the performance of a virtual machine and makes possible many of the ease-of-use features in VMware products

Methodology and Methods

For this project, we used a Toshiba laptop for our analysis of Windows 7 and Windows 10 physical machines. For the first phase, we started by installing Windows 7 on the laptop. Then, after the completion of phase one, Windows 10 was installed. We also used three virtual machines running Windows 7, Windows 10 build 10586, and a Sans SIFT. The build of Windows 10 was important due to compatibility issues during the analysis phase.

After the initial setup of the machines, we decided to create data generation sheets to refer back to in the analysis phase, as well as to ensure that we generated data for the artifacts we chose to analyze. These data generation sheets laid out steps to follow during the data generation phase, such as when to create or modify files. Once the data generation sheets were created, we used the laptop and the Windows virtual machines to generate data for future analysis. We captured data using FTK Imager to take an image of the two physical machines and the two virtual machines. The forensics image was put into EnCase version 7 to parse out the file tree and index all of the files. Indexing the files allows for quick keyword searching through the image. The RAM was also captured using FTK Imager for memory analysis. The resulting file from the RAM capture was run through Volatility to capture various artifacts such as running processes and password hashes.

Equipment Used

Table 1: Hardware

Device	OS Version	Comments
Toshiba Satellite c55t-b5110	Windows 10 Home Edition / Windows 7 Professional	Used for physical Windows data generation/analysis

Table 2: Software

Software	Version	Comments
Microsoft Windows 10	Home Edition	Installed on both the laptop and VM.
Microsoft Windows 7	Windows 7 Professional	Installed on both the laptop and VM
FTK Imager	3.4.2.6	
Encase	7.12.01	
Volatility	2.6	

VMware Analysis

DB Browser for SQLite	3.9.1	
OSForensics	5.2.1003	
LinkParser	1.3	
DCode	4.02a	
VMware Workstation Pro	12.5.0 build-4352439	
VMware vSphere Client	6.0.0 build-2502222	
Sans SIFT	3	

Data Collection

In order to fully document all possible differences found during the analysis of the collected data, as well as creating average user data (such as visiting certain websites, installing programs, changing passwords, and deleting and moving files) a data generation sheet was created *(Appendix 1-4)*. The data for the physical machine analysis of both Windows 7 and 10 was collected from a Toshiba Satellite C55t-B5110 laptop which ran the latest installment of Windows 7 Home Premium and Windows 10 build version 10586. For the virtual machine, Windows 7 Home Premium and Windows 10 build version 10586 were installed using VMware's vSphere.

Analysis

Based on the research we conducted prior to beginning the project, we initially anticipated very little to no differences between the physical machines and VMs, expecting most of the differences to be between Windows 7 and Windows 10.

Data generation for the Windows 7 physical machine began on September 13; for the Windows 7 VM on October 5; the Windows 10 machine on October 19; and the Windows 10 VM on October 26. The same Toshiba laptop was used for all four stages of this project, which was accomplished simply by installing a Windows 10 OS on the device after we finished using Windows 7. The Windows 7 physical machine was wiped completely after use so Windows 10 could be installed. A fake persona named "John Smith" was created for all social media accounts to prevent any personal teammate information from being included in the imaging and memory captures. All aspects of the data gen process followed the steps we outlined in our data gen sheets, in which we recorded the items we created and the date/time each item was completed.

After data generation was completed on a given section, the physical machine or VM had its memory captured and an image generated with FTK Imager. For the physical machines, the image was captured live and was outputted onto an external hard drive. The images for the virtual machines required a different process. Instead of being imaged, the .vmdk files for the virtual machines were copied onto the external hard drive. EnCase has the ability to parse out these files. A variety of forensic analysis tools, including Volatility, EnCase v.7.12.01, DB Browser for SQLite, and the ESEDB Viewer found in Passmark Software's OSForensics software, were used to locate the data and see if there were any differences from the other images and memory captures we created. The artifacts generated were: files moved to the Recycle Bin; LNK files; Prefetch files; Jump Lists; and Google Chrome browser searches.

Results

Windows 7 Physical Machine

LNK Files

The first artifact analyzed on the Windows 7 Physical machine is LNK files. LNK files are shortcut files used by Microsoft Windows to point to an executable file. When these files are parsed out by a tool called LinkParser, important data such as original file location, last modified time, last accessed time, and created time are able to be obtained. This information can tell an investigator where the real file is stored on a disk. In some instances, the LNK file can point to a file on a removable device.

During data generation, a folder was created on the Desktop to store LNK files. In EnCase v.7, the file path "D:\Users\admin\Desktop\LNK" contained the .txt and .lnk files that were created *(Figure 1)*. This folder and subsequent .lnk files are generated in order to test their creation in the "C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Recent" directory *(Figure 2)*. The "Recent" folder shows all current LNK files on a system. Deliberately deleted LNK files were not located within this folder. However, the files created in data generation were present in this folder.

	Name	File Ext	Logical Size	Last Accessed	File Created	Last Written
1	for LNK.txt	txt	11	10/04/17 04:54:22 PM	10/04/17 04:54:22 PM	10/04/17 04:54:38 PM
2	picture2 - Shortcut.lnk	lnk	1,002	10/04/17 04:55:56 PM	10/04/17 04:55:56 PM	10/04/17 04:55:56 PM

Figure 1: LNK files from datagen

	Name	File Ext	Logical Size	Category	Last Accessed	File Created	Last Written
1	AutomaticDestinations		4,096	Folder	09/14/17 04:10:39 PM	09/07/17 05:43:24 PM	09/14/17 04:10:39 PM
2	CustomDestinations		4,096	Folder	09/14/17 05:20:46 PM	09/07/17 05:43:23 PM	09/14/17 05:20:46 PM
3	desktop.ini	ini	432	Windows	09/07/17 05:43:17 PM	09/07/17 05:43:17 PM	09/07/17 05:43:22 PM
4	memdump.7z.lnk	lnk	521	Windows	09/14/17 05:47:04 PM	09/14/17 05:47:04 PM	09/14/17 05:47:04 PM
5	Jump.lnk	lnk	509	Windows	09/14/17 04:10:39 PM	09/14/17 04:10:39 PM	09/14/17 04:10:39 PM
6	same.lnk	lnk	421	Windows	09/14/17 04:35:19 PM	09/14/17 04:35:19 PM	09/14/17 04:35:19 PM
7	LCDI (E).lnk	lnk	223	Windows	09/14/17 04:42:38 PM	09/14/17 04:35:19 PM	09/14/17 04:42:38 PM
8	memes.lnk	lnk	424	Windows	09/14/17 04:35:50 PM	09/14/17 04:35:50 PM	09/14/17 04:35:50 PM
9	Book.lnk	lnk	325	Windows	09/14/17 04:42:22 PM	09/14/17 04:42:22 PM	09/14/17 04:42:22 PM
10	textdoc.lnk	lnk	336	Windows	09/14/17 04:42:38 PM	09/14/17 04:42:38 PM	09/14/17 04:42:38 PM
11	pagefile.7z.lnk	lnk	526	Windows	09/14/17 06:11:24 PM	09/14/17 06:11:24 PM	09/14/17 06:11:24 PM
12	rose-flower-blossom-bloom-39517.lnk	lnk	581	Windows	09/14/17 03:44:14 PM	09/14/17 03:44:14 PM	09/14/17 03:44:14 PM
13	New Text Document.lnk	lnk	578	Windows	09/14/17 03:44:43 PM	09/14/17 03:44:43 PM	09/14/17 03:44:43 PM
14	for thumdnails.lnk	lnk	569	Windows	09/14/17 03:45:15 PM	09/14/17 03:45:15 PM	09/14/17 03:45:15 PM
15	delete me.lnk	lnk	538	Windows	09/14/17 03:46:47 PM	09/14/17 03:46:47 PM	09/14/17 03:46:47 PM
16	for LNK.lnk	lnk	528	Windows	09/14/17 03:48:07 PM	09/14/17 03:48:07 PM	09/14/17 03:48:07 PM
17	chicken.lnk	lnk	430	Windows	09/14/17 03:59:27 PM	09/14/17 03:59:27 PM	09/14/17 03:59:27 PM
18	zipper.txt.lnk	lnk	543	Windows	09/14/17 04:00:33 PM	09/14/17 04:00:33 PM	09/14/17 04:00:33 PM
19	malicious.lnk	lnk	538	Windows	09/14/17 04:04:52 PM	09/14/17 04:04:52 PM	09/14/17 04:04:52 PM

Figure 2 : Recent Folder Containing LNK files

Jump List

The second artifacts analyzed were Jump List files found in "AutomaticDestinations" and "CustomDestinations" directories shown in *Figure 2*. Jump Lists were introduced in the Windows 7 taskbar. They are the menu that appears when the cursor is scrolled over an application in the taskbar. This menu allows for the user to add and remove files as well as open recent files. These files have the extension ".customDestinations-ms" and ".automaticDestinations-ms". During this research project, the tool JumpListExt was used to parse out the ".customDestinations-ms" and ".automaticDestinations-ms" files. During analysis, no CustomDestination files were found by this tool, but 6 AutoDestination files were identified *(Table 3)*.

Table 3: JumpListExt Results

Jump List Files Name	LinkFile Path Affiliations
1b4dd67f29cb1962	C:\Users\John Smith\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms\ C:\Users\John Smith\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms C:\Users\John Smith\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms C:\Users\John Smith\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms C:\Users\admin\Desktop

VMware Analysis

5d69d521de238c3	C:\Users\John Smith\Desktop\chicken.pdf
9b9cdc69c1c24e2b	C:\Users\John Smith\Desktop\New Text Document.txt C:\Users\John Smith\Desktop\for thumdnails.txt C:\Users\John Smith\Desktop\delete me.txt C:\Users\John Smith\Desktop\for LNK.txt C:\Users\John Smith\Desktop\zipper.txt.txt C:\Users\John Smith\Desktop\malicious.txt E:\memes.txt E:\textdoc.txt
7e4dca80246863e3	*Null*
12dc1ea8e34b5a6	C:\Users\John Smith\Desktop\Jump.png
de48a32edcbe79e4	C:\Users\John Smith\Desktop\chicken.pdf

Recycle Bin

The Windows Recycle Bin, most commonly located on a user's desktop, holds files that have been deleted by the user. Each user has their own Recycle Bin on their profile. Files from one user's bin will not be visible in another user's bin on the same machine. Using forensics software like EnCase v7, all of the different user's recycle bin can be identified. *Figure 3* below shows the directory "S-1-5-21-346196833-4268098311-2128948123-1000" under the $Recycle.Bin folder. The numbers that compose the child directory are the user's security identifier, or SID. The "S-1-5-21-346196833-4268098311-2128948123" part of the name pertains to the specific machine while the appending "1000" correlates to the specific user. In this scenario, there is only one Recycle Bin folder due to there only being one user on the system. A computer with multiple users would have a folder for each user.

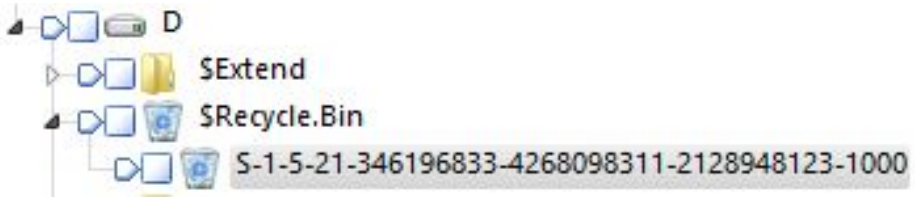
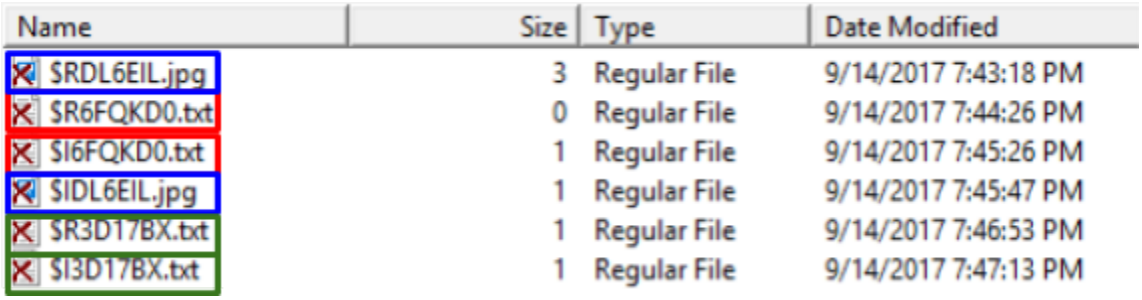


Figure 3: User's Recycle Bin

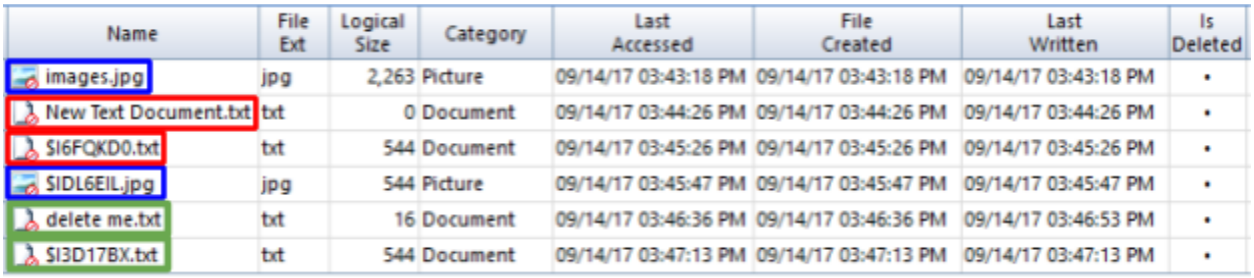
The contents of the $Recycle.Bin folder are shown in *Figure 4* and *Figure 5* below. *Figure 4* is a screenshot from the tool FTK Imager while *Figure 5* is a screenshot from EnCase v7. Both images from the different tools

are included to explain why the results are seemingly different from each other and what a user sees in their own Recycle Bin. The first image, *Figure 4*, is the way the computer views and processes the files. Once a file has been moved to the Recycle Bin folder, it is split into two files. Both files keep the extension from the original file, but the name of the file is altered. One file is labeled "$I" with a few characters after and the second file is labeled with "$R" with the same characters as its sister file. For example, the files outlined in blue below in *Figure 4* show a file named "$RDL6EIL.jpg" and "$IDL6EIL". These files are not readable or in plain text when they separate, but certain tools such as EnCase can parse them out. This is why the output in *Figure 5* is different than that in *Figure 4*. EnCase automatically changes the name of the $R file to the name of the original pre-deleted file.



Name	Size	Type	Date Modified
$RDL6EIL.jpg	3	Regular File	9/14/2017 7:43:18 PM
$R6FQKD0.txt	0	Regular File	9/14/2017 7:44:26 PM
$I6FQKD0.txt	1	Regular File	9/14/2017 7:45:26 PM
$IDL6EIL.jpg	1	Regular File	9/14/2017 7:45:47 PM
$R3D17BX.txt	1	Regular File	9/14/2017 7:46:53 PM
$I3D17BX.txt	1	Regular File	9/14/2017 7:47:13 PM

Figure 4: Contents of $Recycle.Bin in FTK Imager



Name	File Ext	Logical Size	Category	Last Accessed	File Created	Last Written	Is Deleted
images.jpg	jpg	2,263	Picture	09/14/17 03:43:18 PM	09/14/17 03:43:18 PM	09/14/17 03:43:18 PM	•
New Text Document.txt	txt	0	Document	09/14/17 03:44:26 PM	09/14/17 03:44:26 PM	09/14/17 03:44:26 PM	•
$I6FQKD0.txt	txt	544	Document	09/14/17 03:45:26 PM	09/14/17 03:45:26 PM	09/14/17 03:45:26 PM	•
$IDL6EIL.jpg	jpg	544	Picture	09/14/17 03:45:47 PM	09/14/17 03:45:47 PM	09/14/17 03:45:47 PM	•
delete me.txt	txt	16	Document	09/14/17 03:46:36 PM	09/14/17 03:46:36 PM	09/14/17 03:46:53 PM	•
$I3D17BX.txt	txt	544	Document	09/14/17 03:47:13 PM	09/14/17 03:47:13 PM	09/14/17 03:47:13 PM	•

Figure 5: Contents of $Recycle.Bin in EnCase

Browser History

Internet history was the next artifact that was analyzed. Google Chrome was the chosen browser for this project. The main focus was the history.db file within the "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Preferences" directory. This is

a database file that contains URLs that were browsed during datagen, along with correlating date and timestamps of when the website was visited. Search history for the web browser Google Chrome was examined in DB Browser for SQLite. The table "url" shows all of the URLs that were visited during datagen, along with timestamps and a counter for how many times the URL was visited *(Figure 6)*. The tool DCode was used to determine the format of the timestamps listed under the "last_visit_time" column, which it classed as Google Chrome Value. The earliest timestamp translated to September 13th, 2017, 20:18:12 UTC, and the latest being October 04th, 2017, 21:20:28 UTC.

There were no notable differences between any of the tested physical and virtual machines.

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time
	Filter	Filter	Filter	Filter	Filter	Filter
1	69	https://www.youtube.com/watch?v=c_2Ja-OTmGc	Cyber Crime Isn't About Computers: It's About Behavio...	1	0	13151625148104223
2	68	https://notepad-plus-plus.org/download/v7.5.1.html	Notepad++ v7.5.1 - Current Version	1	0	13151624694244578
3	67	https://notepad-plus-plus.org/download/	Notepad++ v7.5.1 - Current Version	1	0	13151624694244578
4	66	https://notepad-plus-plus.org/	Notepad++ Home	1	0	13151624686502525
5	65	https://www.google.com/search?q=notepad%2B%2B&...	notepad++ - Google Search	1	0	13151624679610956
6	64	https://isotropic.org/papers/chicken.pdf	chicken.dvi	1	0	13151624501042557
7	63	https://www.google.com/search?q=chicken.pdf&oq=c...	chicken.pdf - Google Search	1	0	13151624495135107
8	62	https://www.google.com/search?q=chicken&oq=chick...	chicken - Google Search	1	0	13151624480998588
9	61	https://twitter.com/login/error?username_or_email=Jo...	Login on Twitter	3	0	13151624450283107
10	60	https://twitter.com/sessions	(1) Twitter	2	0	13151624450601629
11	59	https://twitter.com/	(1) Twitter	6	1	13151624480815673
12	58	https://my.champlain.edu/	Champlain College	1	1	13151624405206183
13	57	https://www.youtube.com/watch?v=9CemONO6vrY	How the IoT is Making Cybercrime Investigation Easier...	1	0	13151624379498503
14	56	https://www.youtube.com/results?search_query=raje...	rajewski tedx - YouTube	1	0	13151624368111073

Figure 6: Google Chrome History

Windows 7 Virtual Machine

LNK Files

LNK files for the virtual machine are found in the same location as the physical machine: "D:\Users\[username]\AppData\Roaming\Microsoft\Windows\Recent". In *Figure 7* below are the contents of the Recent folder for the virtual machine. In this scenario, there were significantly fewer files in this folder than there were on the physical machine. This is due to inconsistencies in the data generation and does not correlate to differences in format between the physical machine and virtual machine.

VMware Analysis

	Name	File Ext	Logical Size	Last Accessed	File Created	Last Written
1	thumb.lnk	lnk	499	10/04/17 04:52:24 PM	10/04/17 04:52:24 PM	10/04/17 04:52:24 PM
2	Jump.lnk	lnk	398	10/04/17 05:10:06 PM	10/04/17 05:10:06 PM	10/04/17 05:10:06 PM
3	zipper.txt.lnk	lnk	528	10/04/17 05:03:54 PM	10/04/17 05:03:54 PM	10/04/17 05:03:54 PM
4	picture2.lnk	lnk	422	10/04/17 04:52:08 PM	10/04/17 04:52:08 PM	10/04/17 04:52:08 PM
5	delete me.lnk	lnk	523	10/04/17 04:53:24 PM	10/04/17 04:53:24 PM	10/04/17 04:53:24 PM
6	chicken.lnk	lnk	511	10/04/17 05:03:10 PM	10/04/17 05:01:46 PM	10/04/17 05:03:10 PM
7	for LNK.lnk	lnk	513	10/04/17 04:54:30 PM	10/04/17 04:54:30 PM	10/04/17 04:54:30 PM
8	malicious.txt.lnk	lnk	543	10/04/17 05:06:51 PM	10/04/17 05:06:51 PM	10/04/17 05:06:51 PM
9	desktop.ini	ini	432	09/07/17 01:54:15 PM	09/07/17 01:54:15 PM	09/14/17 02:25:16 PM
10	AutomaticDestinations		4,096	10/04/17 05:10:06 PM	09/07/17 01:54:17 PM	10/04/17 05:10:06 PM
11	CustomDestinations		4,096	10/04/17 05:05:46 PM	09/07/17 01:54:17 PM	10/04/17 05:05:46 PM

Figure 7: Recent Files

Jump List

In JumpListExt, the jump list findings were identical to those in the Windows 7 Physical Machine, with the exception of the LinkFile paths affiliated with Jump List file name 9b9cdc69c1c24e2b. In the VM, the results for this particular file included all of those listed for the Physical Machine except for “E:\memes.txt” and “E:\tedoc.txt” (*see Table 3: JumpListExt Results*).

Prefetch Files

Another significant difference between the Windows 7 physical and virtual machines are the contents of the C:\Windows\Prefetch directory. Prefetch files are files that are created on a Windows machine when a program is launched on the system for the first time. The presence of a prefetch file concludes that this program had been run and may still reside on the machine. In this project, the files ”VMTOOLSD.EXE-0AD357E6.pf” and “VMWARESOLTIONSET.EXE-BAE6FDC8.pf” only exist on the Windows 7 virtual machine. These are all files that are associated with VMware and are created at the startup of Windows virtual machines. The physical machine lacked these two files *(Figure 8)*.

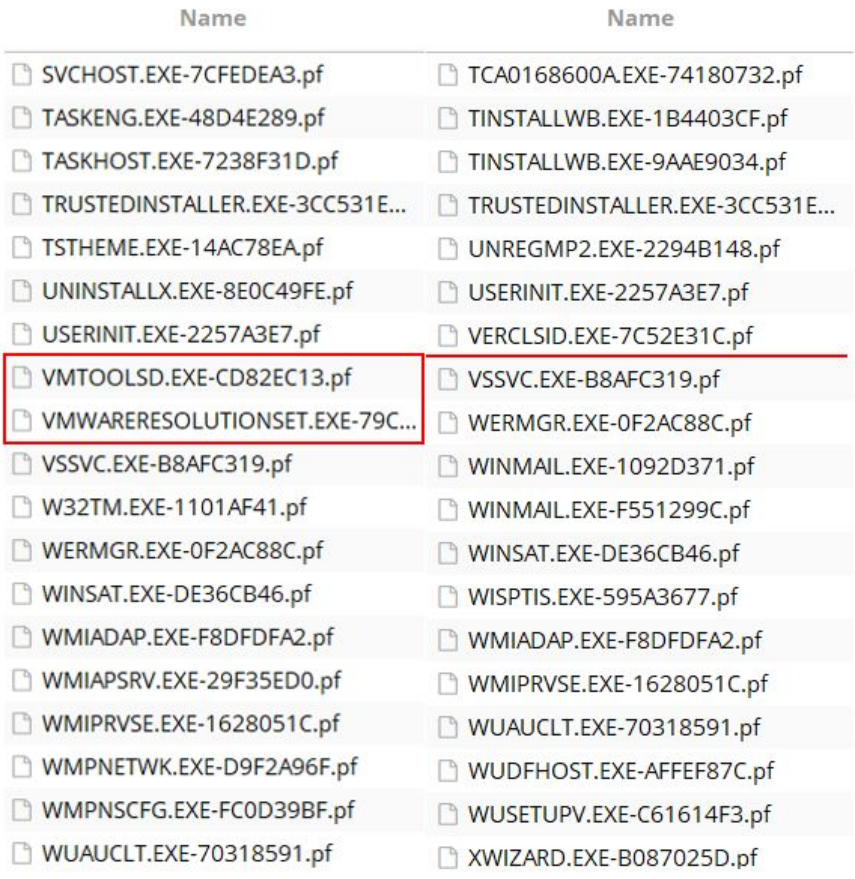


Figure 8: Prefetch Files

Recycle Bin

The files within the Recycle Bin directory for the Windows 7 virtual machine are in the same format of those in the Recycle Bin directory for the Windows 7 physical machine. The files that have been emptied from the Recycle Bin are not shown. The only files that reside in the Recycle Bin are the files that were moved to this directory during data generation. They follow the same format as the $I and $R files, and they all retain the file extension of the original file predeletion.

Browser History

Upon analysis of both the Windows 7 physical machine and virtual machine, there are no notable differences of the format of the History.db file for Google Chrome. The URLs and correlating timestampscontained in this database file are different, but this is due to the different dates and times that data generation for this machine occurred.

Windows 10 Physical Machine

LNK Files

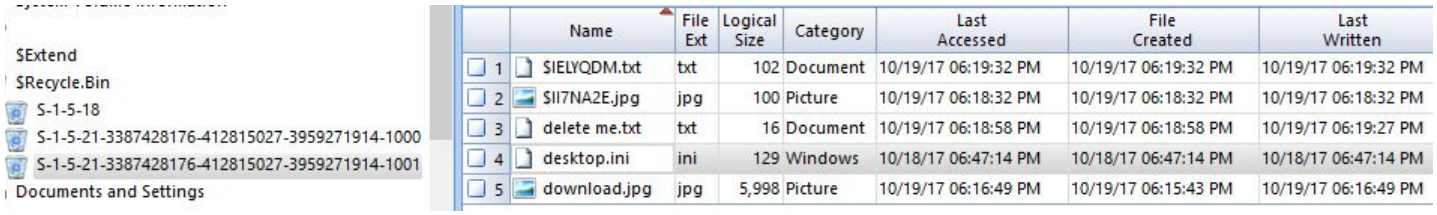
LNK files on Windows 10 are found in the same location as the Windows 7 physical machine and virtual machine, “D:\Users\[username]\AppData\Roaming\Microsoft\Windows\Recent”. The contents of this directory are in the same format as Windows 7 as well. In *Figure 9* below are the contents of the Recent folder for Windows 10.

	Name	File Ext	Logical Size	Category
1	AutomaticDestinations		4,096	Folder
2	CustomDestinations		4,096	Folder
3	chicken.lnk	lnk	467	Windows
4	ms-settingsnetwork.lnk	lnk	154	Windows
5	The Internet.lnk	lnk	104	Windows
6	Network and Sharing Center.l...	lnk	146	Windows
7	Network and Internet.lnk	lnk	116	Windows
8	ms-availablenetworks.lnk	lnk	158	Windows
9	Connect to a network.lnk	lnk	436	Windows
10	All Tasks.lnk	lnk	104	Windows
11	desktop.ini	ini	432	Windows
12	AD_FTK_6.2.1.lnk	lnk	958	Windows
13	Downloads.lnk	lnk	448	Windows
14	flower.lnk	lnk	617	Windows
15	thumb.lnk	lnk	532	Windows
16	delete me.lnk	lnk	556	Windows
17	for LNK.lnk	lnk	419	Windows
18	LNK.lnk	lnk	450	Windows
19	malicous.lnk	lnk	551	Windows
20	zipper.txt.lnk	lnk	561	Windows
21	same.lnk	lnk	285	Windows
22	USB Drive (F).lnk	lnk	179	Windows
23	textdoc.lnk	lnk	296	Windows
24	book.lnk	lnk	285	Windows
25	Jump.lnk	lnk	605	Windows

Figure 9: Windows 10 Prefetch Files

Recycle Bin

The Recycle Bin in Windows 10 physical machine is separated into three sections. Items that were recycled during datagen are found in "D:\$Recycle.Bin\S-1-5-21-3387428176-412815027-3959271914-1001". In this scenario, there were two users on the system, resulting in two different Recycle Bin directories being created (*Figure 10)*.



	Name	File Ext	Logical Size	Category	Last Accessed	File Created	Last Written
1	$IELYQDM.txt	txt	102	Document	10/19/17 06:19:32 PM	10/19/17 06:19:32 PM	10/19/17 06:19:32 PM
2	$II7NA2E.jpg	jpg	100	Picture	10/19/17 06:18:32 PM	10/19/17 06:18:32 PM	10/19/17 06:18:32 PM
3	delete me.txt	txt	16	Document	10/19/17 06:18:58 PM	10/19/17 06:18:58 PM	10/19/17 06:19:27 PM
4	desktop.ini	ini	129	Windows	10/18/17 06:47:14 PM	10/18/17 06:47:14 PM	10/18/17 06:47:14 PM
5	download.jpg	jpg	5,998	Picture	10/19/17 06:16:49 PM	10/19/17 06:15:43 PM	10/19/17 06:16:49 PM

Figure 10: Recycle Bin

Browser History

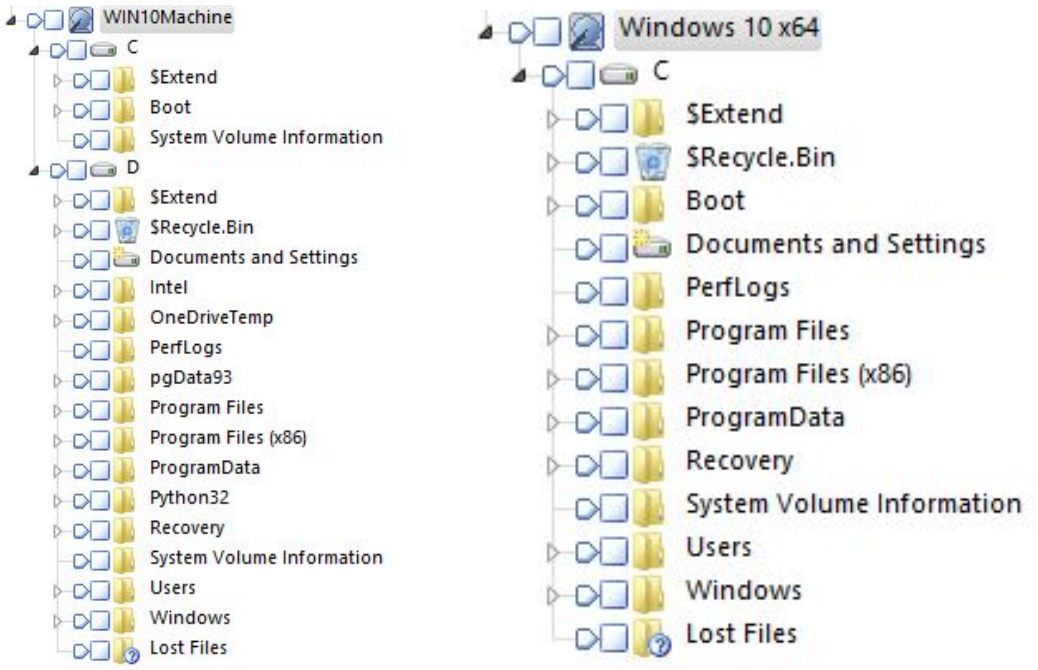
Database files for Google Chrome are found in "D:\Users\smith\AppData\Local\Google\Chrome\User Data\Default\IndexedDB". The Windows 10 Physical Machine contains 6 .leveldb files, including one for Facebook. For unknown reasons, the Windows 10 VM didn't contain this file (*Figure 11*)

	Name	File Ext	Logical Size	Category	Last Accessed	File Created	Last Written
1	https_docs.google.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 05:23:57 PM	10/19/17 02:24:20 PM	10/19/17 05:23:57 PM
2	https_drive.google.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 03:30:04 PM	10/19/17 02:24:09 PM	10/19/17 03:30:04 PM
3	https_twitter.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 06:26:13 PM	10/19/17 06:26:13 PM	10/19/17 06:26:13 PM
4	https_www.facebook.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 06:23:10 PM	10/19/17 06:23:10 PM	10/19/17 06:23:10 PM
5	https_www.google.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 06:44:26 PM	10/19/17 02:55:30 PM	10/19/17 06:44:26 PM
6	https_www.youtube.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 06:24:38 PM	10/19/17 06:24:37 PM	10/19/17 06:24:38 PM

Figure 11: Physical Machine IndexedDB

Windows 10 Virtual Machine

Examining the images for Windows 10 Machine and Windows VM in EnCase v.7, it is apparent that the VM image doesn't have a D: drive. There are fewer folders in the VM than there are in the physical machine, and all folders are on the C: drive. The folders that aren't in the VM are: "Intel", "OneDriveTemp", "pgData93", and "Python32" (*Figure 12)*.



Physical Machine | Virtual Machine

Figure 12: Windows 10 VM has no D: drive

LNK Files

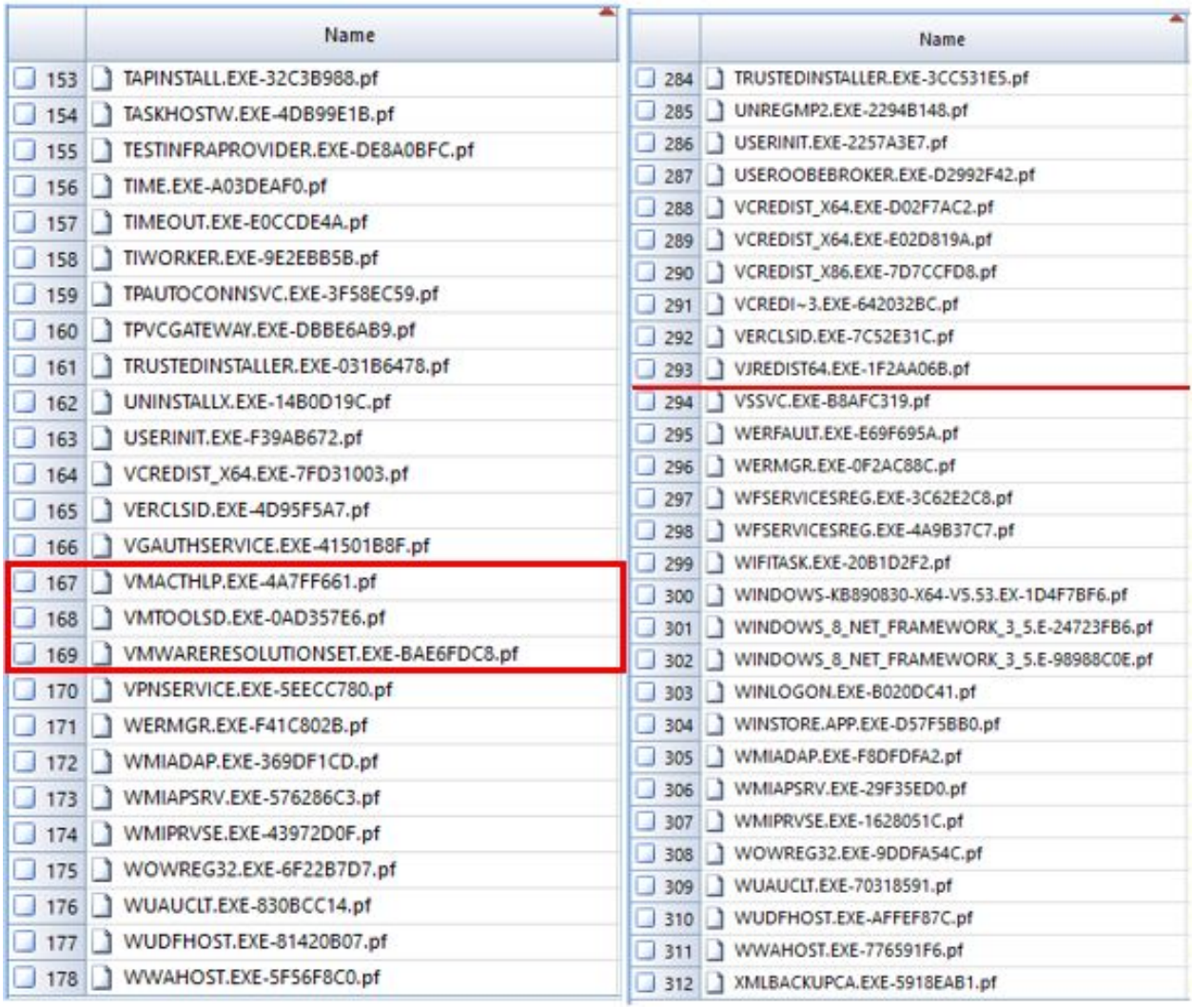
LNK files on the Windows 10 virtual machine are found in the same location as the Windows 7 physical machine and virtual machine, "D:\Users\[username]\AppData\Roaming\Microsoft\Windows\Recent". The contents of this directory are in the same format as Windows 7 as well. In *Figure 13* below are the contents of the Recent folder for the Windows 10 virtual machine.

	Name	File Ext	Logical Size	Category
1	AutomaticDestinations		4,096	Folder
2	CustomDestinations		4,096	Folder
3	for LNK.lnk	lnk	555	Windows
4	desktop.ini	ini	432	Windows
5	delete me.lnk	lnk	565	Windows
6	images.lnk	lnk	626	Windows
7	JUMP.lnk	lnk	614	Windows
8	New Text Document.lnk	lnk	605	Windows
9	rhumb.lnk	lnk	581	Windows
10	LNK.lnk	lnk	453	Windows
11	chicken.lnk	lnk	428	Windows
12	zipper.lnk	lnk	548	Windows
13	malicious.lnk	lnk	565	Windows
14	f-35b-lightning-ii_010-ts600.lnk	lnk	401	Windows
15	(E).lnk	lnk	219	Windows
16	vetstreet.brightspotcdn.lnk	lnk	511	Windows
17	Local Disk (E).lnk	lnk	344	Windows
18	tesxtdoc.lnk	lnk	466	Windows
19	The Internet.lnk	lnk	104	Windows

Figure 13: Windows 10 Virtual Machine Recent Folder

Prefetch Files

The prefetch folder in Windows 10 is similar to Windows 7. Much like on the Windows 7 machines, the files "VMACTHLP.EXE-4A7FF661.pf", "VMTOOLSD.EXE-0AD357E6.pf", and "VMWARESOLTIONSET.EXE-BAE6FDC8.pf" only exist on the Windows 10 virtual machine. These are all files that are associated with VMware and are created at the startup of Windows virtual machines. The physical machine lacked these three files (*Figure 14)*.



	Name
153	TAPINSTALL.EXE-32C3B988.pf
154	TASKHOSTW.EXE-4DB99E1B.pf
155	TESTINFRAPROVIDER.EXE-DE8A0BFC.pf
156	TIME.EXE-A03DEAF0.pf
157	TIMEOUT.EXE-E0CCDE4A.pf
158	TIWORKER.EXE-9E2EBB5B.pf
159	TPAUTOCONNSVC.EXE-3F58EC59.pf
160	TPVCGATEWAY.EXE-DBBE6AB9.pf
161	TRUSTEDINSTALLER.EXE-031B6478.pf
162	UNINSTALLX.EXE-14B0D19C.pf
163	USERINIT.EXE-F39AB672.pf
164	VCREDIST_X64.EXE-7FD31003.pf
165	VERCLSID.EXE-4D95F5A7.pf
166	VGAUTHSERVICE.EXE-41501B8F.pf
167	VMACTHLP.EXE-4A7FF661.pf
168	VMTOOLSD.EXE-0AD357E6.pf
169	VMWARERESOLUTIONSET.EXE-BAE6FDC8.pf
170	VPNSERVICE.EXE-5EECC780.pf
171	WERMGR.EXE-F41C802B.pf
172	WMIADAP.EXE-369DF1CD.pf
173	WMIAPSRV.EXE-576286C3.pf
174	WMIPRVSE.EXE-43972D0F.pf
175	WOWREG32.EXE-6F22B7D7.pf
176	WUAUCLT.EXE-830BCC14.pf
177	WUDFHOST.EXE-81420B07.pf
178	WWAHOST.EXE-5F56F8C0.pf

	Name
284	TRUSTEDINSTALLER.EXE-3CC531E5.pf
285	UNREGMP2.EXE-2294B148.pf
286	USERINIT.EXE-2257A3E7.pf
287	USEROOBEBROKER.EXE-D2992F42.pf
288	VCREDIST_X64.EXE-D02F7AC2.pf
289	VCREDIST_X64.EXE-E02D819A.pf
290	VCREDIST_X86.EXE-7D7CCFD8.pf
291	VCREDI~3.EXE-642032BC.pf
292	VERCLSID.EXE-7C52E31C.pf
293	VJREDIST64.EXE-1F2AA06B.pf
294	VSSVC.EXE-B8AFC319.pf
295	WERFAULT.EXE-E69F695A.pf
296	WERMGR.EXE-0F2AC88C.pf
297	WFSERVICESREG.EXE-3C62E2C8.pf
298	WFSERVICESREG.EXE-4A9B37C7.pf
299	WIFITASK.EXE-20B1D2F2.pf
300	WINDOWS-KB890830-X64-V5.53.EX-1D4F7BF6.pf
301	WINDOWS_8_NET_FRAMEWORK_3_5.E-24723FB6.pf
302	WINDOWS_8_NET_FRAMEWORK_3_5.E-98988C0E.pf
303	WINLOGON.EXE-B020DC41.pf
304	WINSTORE.APP.EXE-D57F5BB0.pf
305	WMIADAP.EXE-F8DFDFA2.pf
306	WMIAPSRV.EXE-29F35ED0.pf
307	WMIPRVSE.EXE-1628051C.pf
308	WOWREG32.EXE-9DDFA54C.pf
309	WUAUCLT.EXE-70318591.pf
310	WUDFHOST.EXE-AFFEF87C.pf
311	WWAHOST.EXE-776591F6.pf
312	XMLBACKUPCA.EXE-5918EAB1.pf

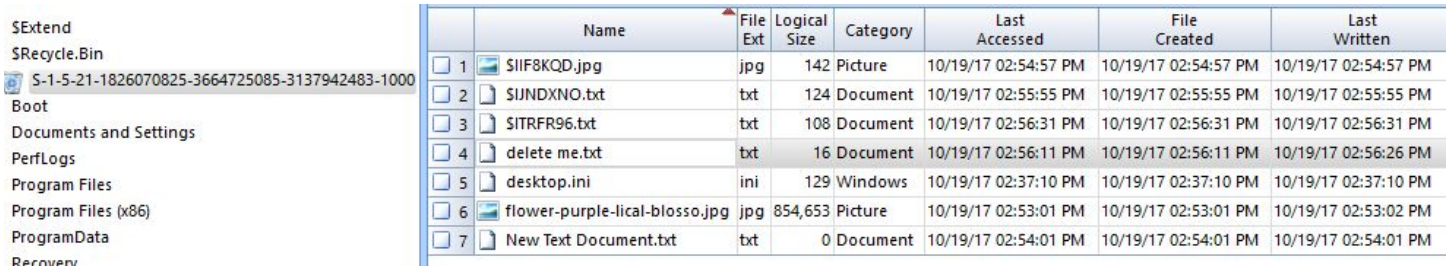
Windows 10 VM

Windows 10 Physical Machine

Figure 14: Physical machine vs. VM prefetch files

Recycle Bin

The items put in the Recycle Bin in the VM are also in a marginally different location than where they were in the physical machine. The VM image has only one folder in the bin, whereas the physical machine had three separate sections. In the VM, the location had an ID ending with 1000, whereas in the physical machine, it was the same ID but ended in 1001 (*Figure 15)*.



	Name	File Ext	Logical Size	Category	Last Accessed	File Created	Last Written
1	$IIF8KQD.jpg	jpg	142	Picture	10/19/17 02:54:57 PM	10/19/17 02:54:57 PM	10/19/17 02:54:57 PM
2	$IJNDXNO.txt	txt	124	Document	10/19/17 02:55:55 PM	10/19/17 02:55:55 PM	10/19/17 02:55:55 PM
3	$ITRFR96.txt	txt	108	Document	10/19/17 02:56:31 PM	10/19/17 02:56:31 PM	10/19/17 02:56:31 PM
4	delete me.txt	txt	16	Document	10/19/17 02:56:11 PM	10/19/17 02:56:11 PM	10/19/17 02:56:26 PM
5	desktop.ini	ini	129	Windows	10/19/17 02:37:10 PM	10/19/17 02:37:10 PM	10/19/17 02:37:10 PM
6	flower-purple-lical-blosso.jpg	jpg	854,653	Picture	10/19/17 02:53:01 PM	10/19/17 02:53:01 PM	10/19/17 02:53:02 PM
7	New Text Document.txt	txt	0	Document	10/19/17 02:54:01 PM	10/19/17 02:54:01 PM	10/19/17 02:54:01 PM

Figure 15: Different Recycle Bin

Browser History

Database files for Google Chrome are found in "C:\Users\Win10_VM\Local\Google\Chrome\User Data\Default\IndexedDB." The Windows 10 Physical Machine contains 6 .leveldb files, including one for Facebook. For unknown reasons, the Windows 10 VM did not contain this file (*Figure 16)*.

	Name	File Ext	Logical Size	Categor	Last Accessed	File Created	Last Written
1	https_docs.google.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 03:40:44 PM	10/19/17 03:39:36 PM	10/19/17 03:40:44 PM
2	https_drive.google.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 03:42:51 PM	10/19/17 03:39:31 PM	10/19/17 03:42:51 PM
3	https_twitter.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 03:13:47 PM	10/19/17 03:13:47 PM	10/19/17 03:13:47 PM
4	https_www.google.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 03:37:23 PM	10/19/17 02:46:37 PM	10/19/17 03:37:23 PM
5	https_www.youtube.com_0.indexeddb.leveldb	leveldb	4,096	Folder	10/19/17 03:08:01 PM	10/19/17 03:08:01 PM	10/19/17 03:08:01 PM

Figure 16: Windows 10 VM IndexedDB

Conclusion

Four different machines have been analyzed to answer the question, “What is the difference between a virtual machine and a physical machine?”. Overall, there are no major differences between the artifacts found; however there are a few minor ones. First, VMware Tools is installed on the virtual machine, resulting in the creation of a prefetch file for this application. We found that the prefetch file was only located on the Windows 7 and Windows 10 virtual machine. This file was not present on the Windows physical machines because VMware Tools can only be used on a virtual machine. Only VMware was tested for this project, therefore this may not be the case for all virtual machine platforms. These differences in Windows artifacts would allow someone to distinguish a physical machine from a virtual machine.

Further Work

Upon completion of this project, there were a few items the team did not have time to complete. These are interesting aspects that would provide a research project for the future, or another team. The first item is testing to see what the resulting artifacts are of connecting a Windows 10 phone to a Windows 10 computer. Windows 10 allowed for a user to receive and send messages from their smartphones on their desktop. There is possibility for text messages, photos, or files to be saved to the machine. The second item on the list for further work is analyzing .vmem files from suspended virtual machines for additional forensic artifacts. During this project, we did not analyze the .vmem file, but pulled the whole virtual machine file into EnCase for analysis. The .vmem file might contain different information. Lastly, there is an opportunity for this team or another team to create a profile for the latest version of Windows 10 OS in Volatility. Volatility does not have support for the most recent builds of Windows 10 installed on their tool. While Volatility may be able to run on Windows 10, memory captures from newer builds of Windows 10 can not be analyzed.

Appendix

Appendix 1: Windows 7 Physical Machine Data Generation Sheet

Action / "Body"	Date (mm/dd/yy hh:mm)
Event Logs	9/14/2017 EST
Start machine	3:33 PM
Log into the machine	3:36 PM
Wait a few minutes, log off the machine	3:38 PM
Wait a few minutes, log on the machine	3:41 PM
Thumbnails	9/14/2017 EST
Drag and drop picture 1 from the internet onto the Desktop	3:43 PM
Right click on picture 2 from Google, click "save as" and save to the Desktop	3:44 PM
Create a new text file on Desktop named "thumb" with "this is for thumbnails" written in it. (Make sure to save it)	3:45 PM
Delete the picture 1 image.	3:45 PM
Recycle Bin	
Create a new text file called "delete me" on Desktop, with "delete this file" written in it	3:47 PM
Delete the text file "delete me"	3:47 PM
LNK	
Create a text file named "for LNK" with "random text" written in it	3:48 PM
Create a folder on the Desktop named "LNK"	3:49 PM
Put the text file inside the folder	3:49 PM
Right click on the text file and click "create shortcut" - put that short cut on the desktop	3:49 PM

Right click on picture 2 and create a shortcut - place the short cut in the folder	3:50 PM
Google Chrome	
Got to gmail.com and log-in to fake gmail account	3:52 PM
Go to http://facebook.com/ and log-in to account.	3:53 PM
Post a status	3:54 PM
Go to http://youtube.com/	3:55 PM
Search 'rajewski tedx' on YouTube	3:55 PM
Click on "rajewski tedx"	3:55 PM
Go to http://my.champlain.edu	3:56 PM
Go to http://twitter.com/ and log-in	3:57 PM
Tweet "test tweet"	3:58 PM
Google chicken.pdf	3:58 PM
Click on the first link	3:59 PM
Download chicken.pdf	3:59 PM
Prefetch	
Open chicken.pdf	3:59 PM
Create a new text file named zipper.txt on Desktop	4:00 PM
Open zipper.txt with notepad	4:00 PM
Open zipper.txt with notepad++	4:04 PM
Create a new text file named malicious.txt	4:04 PM
Open malicious.txt with notepad	4:04 PM
Open malicious.txt with notepad++	4:04 PM
JumpList	
Create a picture in paint - draw whatever you want (needs to be appropriate)	4:10 PM
Save it to the Desktop - name it "Jump"	4:10 PM

USB	
Plug a USB in	4:34 PM
Drag thisisfine.jpg onto the desktop	4:35 PM
Open same.jpg from the USB	4:35 PM
Drag memes.txt to Desktop	4:35 PM
Remove the USB	4:40 PM
Insert a new USB	4:41 PM
Dragged fluffy.jpg to Desktop	4:41 PM
Open book.jpg file from USB	4:42 PM
Open textdoc.txt	4:42 PM
Remove the USB	4:43 PM
Volume Shadow Copies	
Cortana/ Windows Search History	
In the search bar, search "notepad"	4:47 PM
Search "google"	4:47 PM
Search "adobe"	4:47 PM
Search "internet explorer"	4:47 PM
Memory	
Capture memory using FTK Imager	Start: 4:50 PM, End: 5:00PM

Appendix 2: Windows 7 Virtual Machine Data Generation Sheet

Action / "Body"	Date (mm/dd/yy hh:mm)
Thumbnails	**10/4/17**
Drag and drop picture 1 from the Internet onto the Desktop	4:51
Right click on picture 2 from Google, click "save as" and save to the Desktop	4:52
Create a new text file on Desktop named "thumb" with "this is for thumbnails" written in it (make sure to save it)	4:52
Delete the picture 1 image.	4:52
Recycle Bin	**10/4/17**
Create a new text file called "delete me" on Desktop, with "delete this file" written in it	4:53
Delete the text file "delete me"	4:53
LNK	**10/4/17**
Create a text file named "for LNK" with "random text" written in it	4:54
Create a folder on the Desktop named "LNK"	4:54
Put the text file inside the folder	4:55
Right click on the text file and click "create shortcut" - put that short cut on the desktop	4:55
Right click on picture 2 and create a shortcut - place the shortcut in the folder	4:55
Google Chrome	**10/4/17**
Got to gmail.com and log-in to fake gmail account	4:57
Go to http://facebook.com/ and log-in to account	4:58
Post a status	4:58
Go to http://youtube.com/	4:59
Search 'rajewski tedx' on YouTube	4:59
Click on 'rajewski tedx'	4:59
Go to http://my.champlain.edu	5:00
Go to http://twitter.com/ and log-in	5:00

Tweet "test tweet"	5:01
Google chicken.pdf	5:01
Click on the first link	5:01
Download chicken.pdf	5:01
Prefetch	**10/4/17**
Open chicken.pdf	5:02
Create a new text file named zipper.txt on Desktop	5:03
Open zipper.txt with notepad	5:03
Open zipper.txt with notepad++	5:06
Create a new text file named malicious.txt	5:06
Open malicious.txt with notepad	5:06
Open malicious.txt with notepad++	5:06
JumpList	**10/4/2017**
Create a picture in paint - draw whatever you want (needs to be appropriate)	5:10
Save it to the Desktop - name it "Jump"	5:10
USB	
Plug a USB in	5:33
Drag thisdoggo.jpg onto the desktop	5:33
Open majestic.jpg from the USB	5:34
Drag aloha.txt to Desktop	5:34
Dragged floofball.jpg to Desktop	5:35
Open hey.jpg file from USB	5:35
Open textdocument.txt	5:35
Remove BOTH the USB	5:35

Appendix 3: Windows 10 Physical Machine Data Generation Sheet

Action / "Body"	Date (mm/dd/yy hh:mm)
Thumbnails	
Drag and drop picture 1 from the Internet onto the Desktop	6:15
Right click on picture 2 from Google, click "save as" and save to the Desktop	6:17
Create a new text file on Desktop named "thumb" with "this is for thumbnails" written in it (make sure to save it)	6:18
Delete the picture 1 image	6:18
Recycle Bin	
Create a new text file called "delete me" on Desktop, with "delete this file" written in it	6:19
Delete the text file "delete me"	6:19
LNK	
Create a text file named "for LNK" with "random text" written in it	6:20
Create a folder on the Desktop named "LNK"	6:20
Put the text file inside the folder	6:20
Right click on the text file and click "create shortcut" - put that short cut on the desktop	6:21
Right click on picture 2 and create a shortcut - place the shortcut in the folder.	6:21
Google Chrome	
Got to gmail.com and log-in to fake gmail account	6:22
Go to http://facebook.com/ and log-in to account.	6:23
Post a status	6:24
Go to http://youtube.com/	6:24
Search 'rajewski tedx' on YouTube	6:25

Click on 'rajewski tedx'	6:25
Go to http://my.champlain.edu	6:25
Go to http://twitter.com/ and log-in	6:25
Tweet "test tweet"	6:26
Google chicken.pdf	6:26
Click on the first link	6:26
Download chicken.pdf	6:27
Prefetch	
Open chicken.pdf	6:27
Create a new text file named zipper.txt on Desktop	6:28
Open zipper.txt with notepad	6:28
Open zipper.txt with notepad++	6:28
Create a new text file named malicious.txt	6:29
Open malicious.txt with notepad	6:29
Open malicious.txt with notepad++	6:29
Wait a few minutes, log off the machine	6:30
JumpList	
Create a picture in paint - draw whatever you want (needs to be appropriate)	6:32
Save it to the Desktop - name it "Jump"	6:33
USB	
Plug a USB in	6:34
Drag thisisfine.jpg onto the desktop	6:34
Open same.jpg from the USB	6:35
Drag memes.txt to Desktop	6:35
Dragged fluffy.jpg to Desktop	6:35
Open book.jpg file from USB	6:36
Open textdoc.txt	6:36

Remove the USB	6:36
Cortana/ Windows Search History	
In the search bar, search "notepad"	6:36
Search "google"	6:37
Search "what time is it"	6:37
Search "hi cortana"	6:37
Memory	
Capture memory using FTK Imager	6:40

Appendix 4: Windows 10 Virtual Machine Data Generation Sheet

Action / "Body"	Date (mm/dd/yy hh:mm)
Thumbnails	10/19/2017
Drag and drop picture 1 from the Internet onto the Desktop	2:53 PM
Right click on picture 2 from Google, click "save as" and save to the Desktop	2:53 PM
Create a new text file on Desktop named "thumb" with "this is for thumbnails" written in it (make sure to save it)	2:54 PM
Delete the picture 1 image.	2:54 PM
Recycle Bin	
Create a new text file called "delete me" on Desktop, with "delete this file" written in it	2:56 PM
Delete the text file "delete me"	2:56 PM
LNK	
Create a text file named "for LNK" with "random text" written in it	2:56 PM
Create a folder on the Desktop named "LNK"	2:57 PM
Put the text file inside the folder	2:57 PM

Right click on the text file and click "create shortcut" - put that shortcut on the desktop	2:57 PM
Right click on picture 2 and create a shortcut - place the shortcut in the folder.	2:57 PM
Google Chrome	
Go to gmail.com and log-in to fake gmail account	3:00 PM
Go to http://facebook.com/ and log-in to account.	3:07 PM
Post a status	3:08 PM
Go to http://youtube.com/	3:09 PM
Search 'rajewski tedx' on YouTube	3:09 PM
Click on 'rajewski tedx'	3:10 PM
Go to http://my.champlain.edu	3:12 PM
Go to http://twitter.com/ and log-in	3:13 PM
Tweet "test tweet"	3:14 PM
Google chicken.pdf	3:16 PM
Click on the first link	3:17 PM
Download chicken.pdf	3:17 PM
Prefetch	
Open chicken.pdf	3:17 PM
Create a new text file named zipper.txt on Desktop	3:18 PM
Open zipper.txt with notepad	3:18 PM
Open zipper.txt with notepad++	3:18 PM
Create a new text file named malicious.txt	3:18 PM
Open malicious.txt with notepad	3:18 PM
Open malicious.txt with notepad++	3:18 PM
~~Wait a few minutes, log off the machine~~	
JumpList	
Create a picture in paint - draw whatever you want (needs to be appropriate)	3:20 PM

Save it to the Desktop - name it "Jump"	3:20 PM
USB	
Plug a USB in	3:23 PM
Drag bcd.txt onto the desktop	3:23 PM
Open text.txt from the USB	3:24 PM
Drag random Text.txt to Desktop	3:24 PM
Remove the USB	3:24 PM
Insert a new USB	3:25 PM
Drag 6face.jpg to Desktop	3:26 PM
Open vetstreet.jpg file from USB	3:27 PM
Open textdoc.txt	3:27 PM
Remove the USB	3:27 PM
Cortana/ Windows Search History	
In the search bar, search "notepad"	3:27 PM
Search "what time is it"	3:27 PM
Search "dog"	3:31 PM
Search "can pigs fly"	3:32 PM
Memory	
Capture memory using FTK Imager	

References

Ascenzo, W. (2017, October 23). Virtual Machine Forensics Case Study. Retrieved November 08, 2017, from https://www.gillware.com/forensics/blog/digital-forensics-case-study/virtual-machine-forensics-case-study/

Atkinson, T., Flores Cruz, .J (n.d). Digital Forensics on a Virtual Machine. Retrieved November 08,2017, from http://atkison.cs.ua.edu/papers/ACMSE11_JF.pdf

Hirwani, M., Pan, Y., Stackpole, B., & Johnson, D. (n.d.). Forensic Acquisition and Analysis of VMware Virtual Hard Disks. Retrieved November 08, 2017, from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1300&context=other

Shavers, B. (n.d). Virtual Machines: A Discussion of Virtual Machines Related to Forensics Analysis Retrieved November 08, 2017, from https://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf

Wilson, C. (2017, November 04). Virtual Machine Forensics Using Virtual Machine Email Recovery Tool. Retrieved November 08, 2017, from http://www.dataforensics.org/virtual-machine-forensics/