11-5-2013

A Forensic Comparison: Windows 7 and Windows 8

Peter J. Wilson

A Forensic Comparison: Windows 7 and Windows 8

by

Peter J. Wilson

Committee Members

Doctor Yin Pan

Doctor Sumita Mishra

Professor Harris Weisman

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in

Computer Security and Information Assurance

Rochester Institute of Technology

B. Thomas Golisano College

of

Computing and Information Sciences

11/05/2013

Rochester Institute of Technology

B. Thomas Golisano College

of

Computing and Information Sciences

Master of Science in

Computer Security and Information Assurance

Thesis Approval Form

Student Name: Peter J. Wilson

Thesis Title: A Forensic Comparison: Windows 7 and Windows 8

Thesis Committee

Doctor Yin Pan

Chair

Doctor Sumita Mishra

Committee Member

Professor Harris Weisman

Committee Member

Abstract

Whenever a new operating system or new version of an operating system is released, forensic investigators must re-examine the new operating system or new version. They do so to determine if there are significant differences that will impact and change the way they perform their investigations. With the release of Microsoft's latest operating system, Windows 8, and its update, Windows 8.1, understanding the similarities and differences between Windows 8 and previous operating systems such as Windows 7 is critical. This paper forensically examines Windows 7 and Windows 8 to determine those similarities and differences.

Acknowledgements

This thesis has evolved significantly over the past year. During the slow and often interrupted evolution of this thesis I have come to greatly appreciate those who supported me. I would like to specially thank my mother, Mimi Wilson, and father, Philip Wilson, for their consistent reminders and interest in my research. I would also like to thank my sisters, Jennifer and Kate Wilson, for their gentle nagging and assistance in the review process. Even though it took me far longer than I originally intended to complete my thesis, my family provided the encouragement I needed and helped me find the motivation to finish. I would like to express my sincerest thanks to them.

In addition, I would also like to thank my thesis committee, Doctor Yin Pan, Doctor Sumita Mishra, and Professor Harris Weisman, for their excellent guidance and thoughtful suggestions. Their classes throughout my undergraduate and graduate careers are what sparked my interest in computer forensics.

My close friends Nathan Welshans, Andrew Guirguis, and Thomas Kopchak deserve a measure of thanks. Working side by side with them, in more classes than I can remember, was thoroughly enjoyable. Their knowledge of networking and systems administration helped me to complete courses I never would have been able to on my own.

Finally, I would like to thank the Network Security and Systems Administration department for sponsoring me as a graduate assistant. Without that scholarship I wouldn't have even bothered pursuing a master's degree. Thank you.

Table of Contents

List of Tables

List of Figures

Introduction

As of October 26th, 2012 Microsoft's newest client operating system is Windows 8. While developers, IT professionals, MSDN and TechNet subscribers, and others have had access to the new operating system since August, the general public can now get their hands on Microsoft's latest client operating system. [1] The release of new operating systems brings significant challenges, especially for the forensic community. Since its first Windows operating system in 1985, Microsoft has released several different operating systems. While each iteration of operating system has built upon the success of previous versions, there are also noteworthy differences with each new iteration. These differences provide challenges that forensic examiners must overcome in order to perform their analysis of computer systems.

As with other Microsoft operating systems, Windows 8 follows the pattern of having considerable differences from its predecessor. [2] The most significant difference between Windows 8 and Windows 7 pertains to the user experience. In Windows 8, the start menu, present in all Microsoft operating systems since Windows 95, is entirely replaced with the start screen. [3] However, the addition of the start screen is only a small portion of the changes to the user interface. In addition to the start screen, the user experience has changed significantly by combining the tile based "Modern" style applications and previously used desktop style applications. [4] Some "Modern" applications that are worthy of note are the People App [5]and Internet Explorer 10 [6]. There are many differences between the user experience of Windows 8 and Windows 7; this research explores how those differences impact forensic analysis.

Another major difference between Windows 8 and previous versions of Windows is the ability to use a single user account across multiple PCs through Windows Live. [7] Using a Windows Live account allows synchronization of SkyDrive, Email, Calendar, Contacts, Messaging, and Photos/Videos between PCs that are associated with a Windows Live account. [8] Prior to my research, the impact that this synchronization has on forensic capabilities was unknown, this research determines that impact.

In Windows 8, the previously used Previous Versions and Backup and Recovery feature is deprecated. Instead, Windows 8 utilizes File History, a feature that performs incremental backups of personal files. [9] File History is designed to simplify the data protection process.

What bearing this new feature will have concerning forensics was unknown; this research helped to uncover that.

Needless to say, there are many differences between Windows 8 and previous Microsoft operating systems. My research explores those differences and any influence they have on the forensic process or forensic investigations. My research is primarily focused around the non-live forensic similarities and differences that exist between Microsoft's latest client operating system, Windows 8, and its previous client operating system, Windows 7. This research and its documentation are extremely important because of the limited information regarding Windows 8 forensics.

Literature Review

In order to better understand computer forensics as it pertains to Windows 8, it is worthwhile to explore the research conducted, and papers and articles written relating to the topic. Unfortunately, there are a limited number of resources that cover Windows 8 forensics specifically. Those resources that do cover this topic are by no means comprehensive and very few are purely academic; many of the resources relating to this topic are highly technical industry papers or blog postings. Most of the articles, presentations, or blog postings that I have been able to find only scratch the surface of exploring Windows 8 from a forensic point of view. Despite this, I was able to find a few excellent resources for the basis of my research into Windows 8 forensics.

In Amanda C. F. Thomson's "Windows 8 Forensic Guide", the author explores several forensic aspects of Windows 8 including the new graphical user interface of the operating system, which is designed with touch screen devices in mind. The majority of the paper is focused upon artifacts a forensic examiner might uncover in their examination of a Windows 8 system including the User folder, "Modern" applications and their caches and cookies, the communication application, and several other interesting artifacts. In addition, the paper also contains a section relating to the Windows Registry, a common location for forensic examiners to explore. Throughout the process, Thomson points out some of similarities and some of the differences between the Window 8 artifacts and similar artifacts that may or may not have existed in Windows 7. [10] Thomson's paper provides an excellent beginning for research regarding Windows 8 forensics. It contains a significant amount of information that my research

builds upon. This paper is important to my research because it details some of the similarities and differences regarding artifacts for Windows 8 forensics. My research expands upon the research of Thomson; exploring additional artifacts uncovered though my experimentation process. My research uncovers new artifacts that are not covered in the "Windows 8 Forensic Guide" and details my research findings.

In Ethan Fleisher's blog posts and YouTube videos, "Windows 8 Forensics", key forensic differences between Windows 7 and Windows 8 are explored. The blog posts and videos include the following topics of research: recycle bin properties, USB drive activity, Internet history, event logs, and the file history feature. In some cases, Fleisher determined that there is little to no forensic difference between Windows 7 and Windows 8. One significant finding to note is the differences involved with Internet Explorer 10. The author uncovered that Internet cookies and history files are stored in different locations from the previous version of Windows. Fleisher's LCDI blog posts and YouTube videos provide some basic details pertaining to forensic analysis of a Windows 8 system. [11] While limited, these blog posts helped to provide me with a starting point for setting up my experiments and beginning the analysis process. In addition, I was also able to explore some of the topics that the author planned on studying but never got around to.

An important tool that was extremely useful while performing the forensic analysis of Windows 7 and Windows 8 was the "SANS Windows Artifact Analysis" poster. This poster is something of a quick guide for uncovering evidence of file download, program execution, file opening/creation, file deletion, location, USB/drive usage, account usage, and browser usage. [12] While the poster only contains information for Windows XP and Windows 7, I was able to use the information on the poster to serve as a guide for my analysis. In addition, I was also able to compare my forensic analysis findings of the Windows 8 virtual machine with that of the poster. This poster accelerated my research and helped me to uncover differences between Windows 7 and Windows 8 forensically.

In J. Philip Craiger's article, "Computer Forensic Procedures and Methods", the fundamentals of computer forensics are covered. The article begins by reviewing forensic tools, listing best practices, and outlining first steps for a forensic analysis. The article continues to detail the analysis of a forensic image providing steps and guidance along the way. [13] This is important information; however, the portion of the article of most interest to my research is the section pertaining to the technical analysis of a forensic image. Unfortunately, this article

is written with a focus on Windows XP. This means that this article is primarily useful for providing suggestions for forensic artifacts that may be of interest.

In Josh Brunty's presentation, "Windows 8 A Forensic First Look", the presenter demonstrates some of the forensic findings that researchers at Marshall University have been able to uncover with Microsoft's latest operating system. Brunty begins with a general overview of the operating system along with the new "Modern" graphical interfaces and some of the differences between previous versions of Windows. As he continues his presentation, the file structure of Windows 8 is explored and the many forensic artifacts that are left behind for forensic examiners to locate. There are a few very interesting items that Brunty points out in his presentation. Primarily, that each immersive application has its own registry file and own Internet artifacts (Cache, Cookies, History). This is especially important for the People application which contains information pulled from Twitter, Facebook, Google+, other social media sites, contacts, email, etc. making it easier for forensic investigators to obtain information. [14] Brunty's presentation is significant in relation to my research as it served as a jumping point from which I was able to further extend some of the topics that were not covered or minimally covered by the presentation.

Ken Johnson, through his blog Random Thoughts of Forensics, has several blog posts that are relevant to my research. His post "Windows 8 Forensic Overview" serves as an excellent index for his other blog posts pertaining to the registry, file history, and refresh and recovery options of Windows 8. In one of his blog posts on the Windows 8 registry, Johnson points out the TypedURLs and TypedURLsTime registry keys. These keys are extremely interesting forensic artifacts that could be used by an investigator to determine when specific URLs were visited. In another blog post, Johnson points out that once Windows 8 File History Service is enabled, numerous artifacts are created including event logs, registry settings, configuration files, and even backups of personal directories if selected. [15] Johnson's blog posts are especially important to my research because his research points out that he has only scratched the surface in regards to the registry, file history, and refresh and recovery options. His research gave me a place to start in my comparison of Windows 7 and Windows 8 forensic artifacts. While I've replicated some of his findings in my own research, I have also compared my findings and his findings within Windows 8 to that of Windows 7.

In Rob Lee's SANS blog post, "Windows 7 Computer Forensics", several pertinent topics are discussed. Each of the areas in which Lee provides links to other articles are areas in which I can focus my research for Windows 8. His posting documents the areas of user profiles, Internet Explorer, USB Key Analysis, Defrag Analysis, Timeline Analysis, and Shadow Copy Forensics. All of the research he has uncovered pertains to Windows 7. [16] This is useful to me because rather than replicating other people's research, I can focus on exploring how Windows 8 is forensically similar or different from Windows 7. I can use Lee's documentation and research to compare against my findings in similar areas for Windows 8.

Methodology

Since my thesis focuses on the forensic similarities and differences between Windows 7 and Windows 8, I performed a variety of actions in order to discover those similarities and differences. I designed a network topology, installed software/applications, generated user data, and finally, performed a forensic analysis, on Windows 7 and Windows 8. Through the activities detailed, I was able to determine how the significant similarities and differences between Windows 8 and previous versions of Windows affect forensic analysis in the Results and Comparison section below.

Network Topology

For the network topology, I setup a basic, commercial off the shelf, Netgear Router and a server running Microsoft's Windows Server 2008 R2. The router enabled me to connect the server, and subsequent Virtual Machines, to The Internet and install updates and necessary software. The router was configured to have a Local Area Network (LAN) IP address of 192.168.1.1 with a 24 bit subnet mask and serve as the default gateway for the server. The router was also configured by the Internet Service Provider (ISP) to have a WAN IP address of 69.207.87.120, a 23 bit subnet mask, and a default gateway of 69.207.86.1. Finally, I configured the router to use Google's Domain Name Service (DNS) servers (8.8.8.8 and 8.8.4.4) for providing name resolution. The server enabled me to use VMware Workstation 9 to set up two virtual machines. These virtual machines were configured with Windows 7 Professional and Windows 8 Professional and were connected to the LAN through a VMware Virtual Router that provided Network Address Translation (NAT) to the LAN from the virtual network vmnet8.

Vmnet8 was setup to use the 192.168.106.0 subnet with a 24 bit subnet mask. The virtual network was configured with a gateway of 192.168.206.254 and set to auto detect DNS servers. The Windows 7 virtual machine received a MAC address of 00:0C:29:B3:BB:88 and an IP address of 192.168.106.128 while the Windows 8 virtual machine received a MAC address of 00:0C:29:7D:FC:55 and an IP address of 192.168.106.129. The entire topology is detailed in Figure 1.

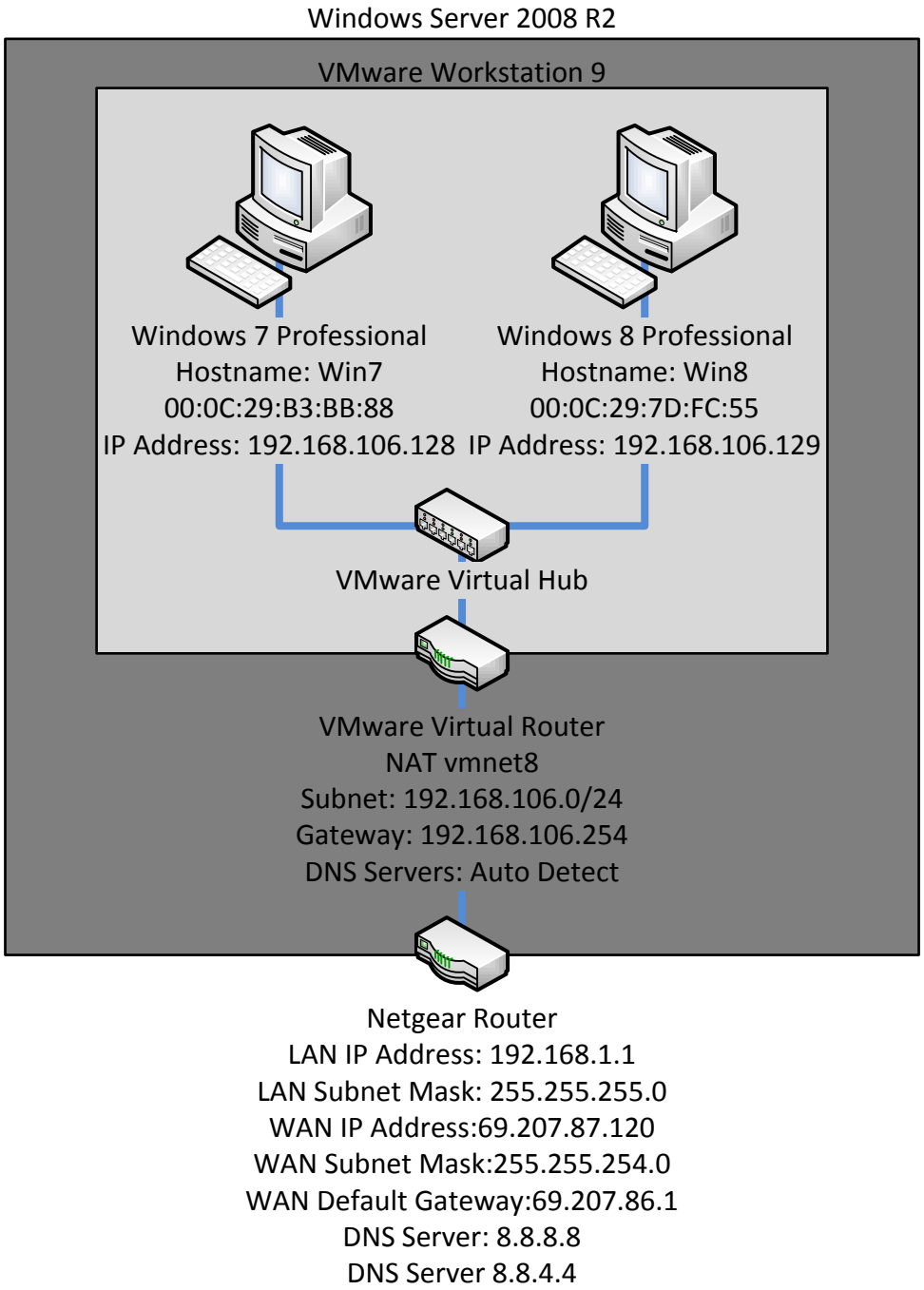


Figure 1 Entire Network Topology

In addition to the network topology above, I also set up a virtual machine running Windows 7 on the Remote Laboratory Emulation System (RLES) for Rochester Institute of Technology (RIT). RLES uses VMware's vCloud to provide virtual machines to students and professors. Using this system, I created a virtual machine that I would use for forensic analysis of

the virtual machine files from both Windows 7 and Windows 8. The topology for the forensic analysis virtual machine can be seen in Figure 2.

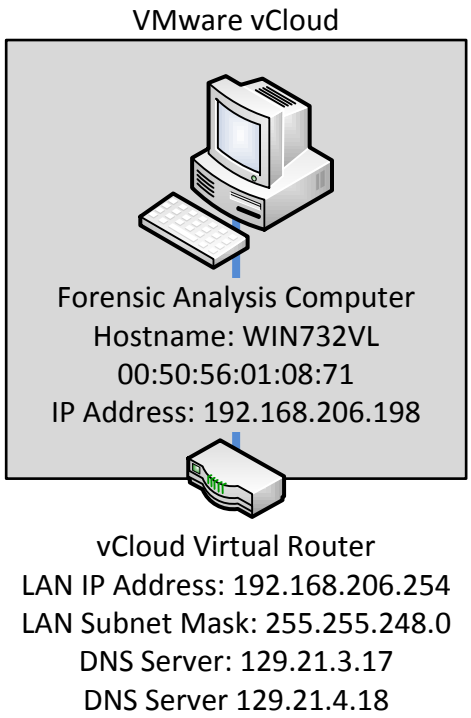


Figure 2 Forensic Network Topology

Virtual Machine Settings

In addition to the network topology, the virtual machines were also configured with specific settings. Each virtual machine was given a name of the format Windows <7/8> depending on which operating system was installed. Each virtual machine was stored on an NTFS partition (P:\Virtual Machines), within its own folder on the server, and was configured to use VMware Workstation version 9.0. The virtual machines were installed with the 64 bit versions of their respective operating systems and configured with a 40 Gigabyte (GB) pre-allocated hard disk and 1024 Megabytes (MB) of memory. The virtual machines were also configured with the NAT network adapter allowing them to connect to the vmnet8 network and the LAN through the VMware virtual router, and ultimately The Internet through the Netgear router. The new virtual machine wizard for each virtual machine can be seen in Figure 3 and Figure 4.

Windows 7

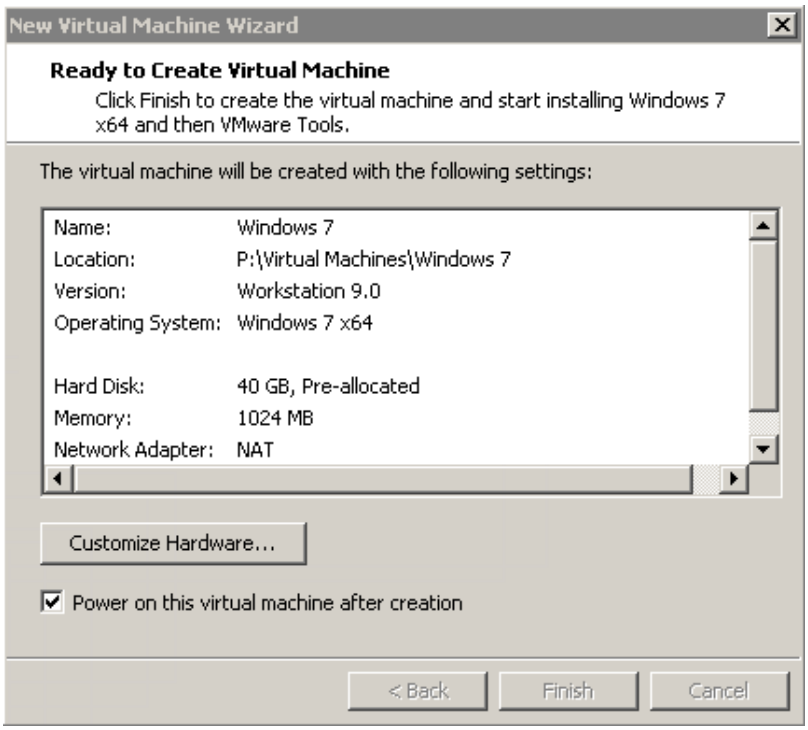


Figure 3 Windows 7 Virtual Machine Settings

Windows 8

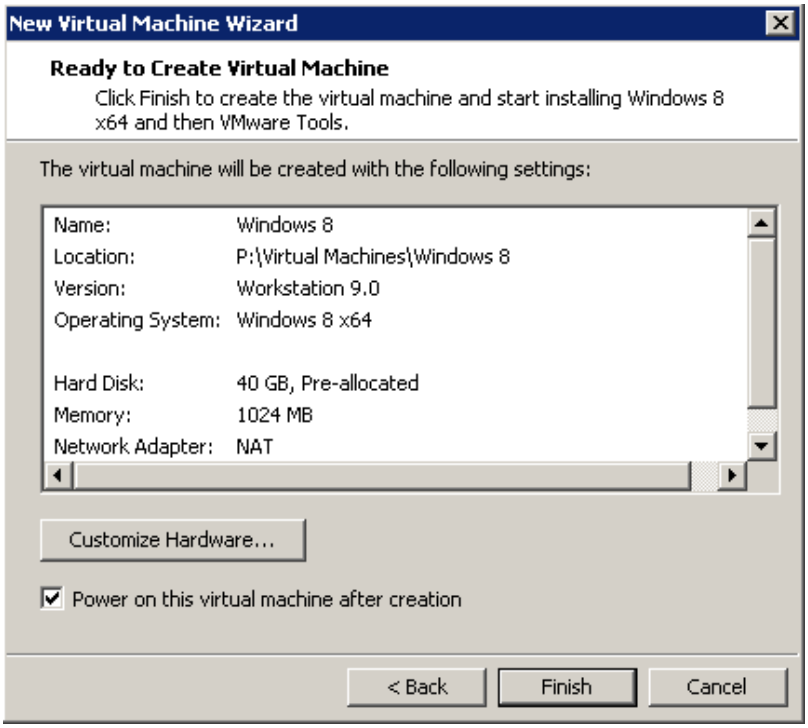


Figure 4 Windows 8 Virtual Machine Settings

Installed Software

In regards to the software and/or applications installed on the virtual machines, I attempted to limit the programs installed to those that are commonly used. In fact, very little software was actually needed to create user data. In most cases, the software that came preinstalled with the operating systems was adequate. Table 1 details the software that I installed on the virtual machines along with preinstalled software that I used frequently throughout the data generation process.

Table 1 Virtual Machine Software

Frequently Used Installed Software		
Software Type	**Windows 7**	**Windows 8**
Web Browser	Firefox	Firefox
	Chrome	Chrome
Email Application	Windows Live Mail 2012	
Frequently Used Preinstalled Software		
Web Browser	Internet Explorer	Internet Explorer Desktop
		Internet Explorer App
Text Editor	Notepad	Notepad
Email Application		Windows 8 Email App

As you can see, on Windows 7 I needed to install three applications while on Windows 8 I only needed to install two. This is because Windows 7 does not come with a preinstalled email application whereas Windows 8 does. In addition, any software or applications that were installed or used were setup or configured with the default configurations. This means that wherever possible, I accepted defaults during installation and/or did not make any changes to the settings.

User Data

Having valid user data was very important for the research that I conducted. As such, each virtual machine was used for ten days over a period of fourteen days to perform common basic tasks. I wanted to have user data that was the result of common computer usage; things like web browsing, email sending, file creation, etc. that a common user would perform frequently on their computer. In order to create this user data I created accounts and then used those accounts in my data generation process.

Accounts

For the purpose of creating user data, I created a total of eight accounts. I created two email accounts for each operating system, one Facebook account for each operating system, and one Twitter account for each operating system. Table 2 shows more detailed information regarding the accounts I created.

Table 2 Accounts Created for Virtual Machines

Created Accounts	
Windows 7	**Windows8**
Email:	**Email:**
PeterWilson.Win7@gmail.com	PeterWilson.Win8@gmail.com
PeterWilson.Win7@live.com	PeterWilson.Win8@live.com
Facebook: facebook.com/windowsseven.forensics	**Facebook:** facebook.com/windowseight.forensics
Twitter:	**Twitter:**
twitter.com/win7forensics	twitter.com/win8forensics

Data Generation

The activities that I performed from 04/21/2013 to 05/04/2013 included file creation/deletion/download, Internet browsing, sending/replying/forwarding email with and without attachments, and performing a variety of social media actions such as posting/sharing/commenting/liking on Facebook and tweeting/retweeting/replying on Twitter. In addition, I occasionally attempted to use some of the new features and applications available in Windows 8. Table 3 and Table 4 serve as a complete listing of the activities that I performed over the data generation period including the days that I performed them on. While I was performing these tasks, I also kept a detailed log of actions performed for later comparison with my forensic analysis findings (see Appendix A).

Table 3 Windows 7 Data Generation Activities

Windows 7 Date/Activity	04/21/2013	04/23/2013	04/24/2013	04/25/2013	04/26/2013	04/28/2013	05/01/2013	05/02/2013	05/03/2013	05/04/2013
Created Daily File in C:\Users\Windows7\Documents\		X		X	X	X	X	X	X	
Created Attachment File in C:\Users\Windows7\Documents\			X				X		X	
Created Deleted File in C:\Users\Windows7\Documents\			X			X	X		X	
Downloaded File to C:\Users\Windows7\Downloads\		X		X	X		X		X	
Deleted File in C:\Users\Windows7\Documents\			X			X	X	X	X	
Deleted File in C:\Users\Windows7\Downloads\				X			X		X	X
Empty the Recycle Bin					X					X
Browsed to the Featured Wikipedia Article using all Browsers	X	X	X	X	X	X	X	X	X	X
Browsed to RIT's Top News Stories for the day using all Browsers	X	X	X	X	X	X	X	X	X	X
Browsed to Facebook, Automatically Logged In using all Browsers	X	X	X	X	X	X	X	X	X	X
Browsed to Twitter, Automatically Logged In using all Browsers	X	X	X	X	X	X	X	X	X	X
Sent email to other 3 accounts from the Windows7 Live Account	X				X					
Sent email to other 3 accounts from the Windows7 Gmail Account		X		X				X		X
Sent email with attachments to other 3 accounts from the Windows7 Live Account			X				X		X	
Sent email with attachments to other 3 accounts from the Windows7 Gmail Account						X				
Reply to Daily Email using Windows Live Mail 2012 to Original Sender				X	X		X		X	
Forward Daily Email using Windows Live Mail 2012 to Original Sender				X	X		X		X	
Posted Daily Post on Facebook	C	F	IE	C	F	IE	C	F	IE	IE
Shared Post of Facebook	IE	C	F		C	F				F
Shared Photo on Facebook				IE			IE	C	F	
Comment on Daily Facebook Post				C	F	IE	C	F	IE	IE
Like Daily Facebook Post					F	IE	C	F	IE	IE
Tweeted Daily Tweet on Twitter	F	IE	C	F	IE	C	F	IE	C	C
Retweeted Tweet on Twitter		IE	C	F	IE	C	F	IE	C	C
Reply to Daily Tweet on Twitter				IE	C	F	IE	C	F	F
Checked for Updates			X	X			X		X	X
Installed Important Updates										
Table										
C = Chrome										
IE = Internet Explorer										
IE App = Internet Explorer App										
F = Firefox										

Table 4 Windows 8 Data Generation Activities

Windows 8 Date/Activity	04/21/2013	04/23/2013	04/24/2013	04/25/2013	04/26/2013	04/28/2013	05/01/2013	05/02/2013	05/03/2013	05/04/2013
Created Daily File in C:\Users\Windows7\Documents\		X		X	X	X	X	X	X	X
Created Attachment File in C:\Users\Windows7\Documents\			X				X		X	
Created Deleted File in C:\Users\Windows8\Documents\			X			X	X		X	
Downloaded File to C:\Users\Windows8\Downloads\		X		X	X		X		X	
Deleted File in C:\Users\Windows8\Documents\			X			X	X	X	X	
Deleted File in C:\Users\Windows8\Downloads\				X			X		X	X
Empty the Recycle Bin					X					X
Browsed to the Featured Wikipedia Article using all Browsers	X	X	X	X	X	X	X	X	X	X
Browsed to RIT's Top News Stories for the day using all Browsers	X	X	X	X	X	X	X	X	X	X
Browsed to Facebook, Automatically Logged In using all Browsers	X	X	X	X	X	X	X	X	X	X
Browsed to Twitter, Automatically Logged In using all Browsers	X	X	X	X	X	X	X	X	X	X
Sent email to other 3 accounts from the Windows8 Live Account	X				X					
Sent email to other 3 accounts from the Windows8 Gmail Account		X		X				X		X
Sent email with attachments to other 3 accounts from the Windows8 Live Account			X				X		X	
Sent email with attachments to other 3 accounts from the Windows8 Gmail Account						X				
Reply to Daily Email using Mail App to Original Sender				X	X		X		X	
Forward Daily Email using Mail App to Original Sender				X	X		X		X	
Posted Daily Post on Facebook	C	People App	IE App	C	F	People App	C	F	People App	
Shared Post of Facebook	IE		F		C	IE App				
Shared Photo on Facebook				IE App			IE App	C	F	IE App
Comment on Daily Facebook Post				C	F	People App	IE App	F	People App	C
Like Daily Facebook Post					F	People App	IE App	F	People App	C
Tweeted Daily Tweet on Twitter	F	People App	C	F	IE App	People App	F	IE	People App	F
Retweeted Tweet on Twitter		People App	C	F	IE App	People App	IE App	IE	People App	F
Reply to Daily Tweet on Twitter				People App	C	People App	IE	C	People App	IE App
Opened and Browsed through "What's New" in the People App	X				X		X			
Viewed Unread Notifications in the People App	X				X		X			
Viewed Weather Information through the Weather App	X		X			X				
Got Directions using Map App			X				X			
Vewed Finance Information through Finance App					X		X			
Viewed Sports Information through Sports App					X		X			
Checked for Updates			X	X			X		X	X
Installed Important Updates			X	X					X	X
Table										
C = Chrome										
IE = Internet Explorer										
IE App = Internet Explorer App										
F = Firefox										

Forensic Analysis

After fourteen days of generating user data, I began the process of forensic examination. I drew upon the knowledge I obtained from my coursework, specifically undergraduate class, Computer System Forensics, and graduate class, Advanced Computer Forensics to examine the virtual hard disks of both virtual machines. To complete my examination, I followed a standard forensic investigation procedure of Data Collection, Data Preservation, Data Analysis, and Reporting.

Data Collection

In order to collect the data stored on the Windows 7 and Windows 8 virtual machines, I first needed to acquire forensic images of the hard disks. Fortunately, AccessData's Forensic Toolkit, Guidance Software's EnCase Forensic, and Magnet Forensic's Internet Evidence Finder have the ability to examine VMware Virtual Machine Disks with the .vmdk file format. This was extremely fortunate because I did not have to worry about data acquisition and converting the images into special formats.

After I shut down the virtual machines, I proceeded to obtain hashes for Windows 7-flat.vmdk and Windows 8-flat.vmdk, the virtual machine disks from both Windows 7 and Windows 8 respectively. I used NirSoft's HashMyFiles [17] to calculate MD5, SHA1, and SHA-256 hashes of relevant virtual machine files. The program took some time to run as the files were rather large (approximately 40GB) but ultimately was able to calculate the needed hashes:

Table 5 Initial Hash Calculations

Filename	MD5	SHA1	SHA-256	Full Path	Modified Time	Created Time	File Size
Windows 7-flat.vmdk	8800bcad1a173fd07a1b74f11c8545b9	81290ce989246c28d140092a46f60e1e91d1d89f	71d09c2280225235d18b30f5599ae37fef4d2f38a98499c615f05fc6632e2f11	F:\Virtual Machines\Windows 7\Windows 7-flat.vmdk	5/4/2013 3:59:42 PM	5/7/2013 9:12:47 AM	42949672960
Windows 8-flat.vmdk	752594eab4acf342891d7fe4421e4777	9ca91f650de285d2af8f863b1c2efeee7310ea34	3643019d5ed03d6ee4a245183e3897eb665a0d392dbf5504a4b51f346bdfefaa	F:\Virtual Machines\Windows 8\Windows 8-flat.vmdk	5/4/2013 3:59:25 PM	5/7/2013 9:51:52 AM	42949672960

Since I was going to be using a forensic virtual machine configured with EnCase, FTK, and a variety of other forensic tools located on RIT's Remote Laboratory Emulation System (RLES), I needed to transfer the virtual machines files from the Windows Server 2008 R2 server to the forensic virtual machine. In order to do so, I used 7-Zip [18], an open source file archiver to compress the virtual machines files from approximately 80GB to approximately 17GB:

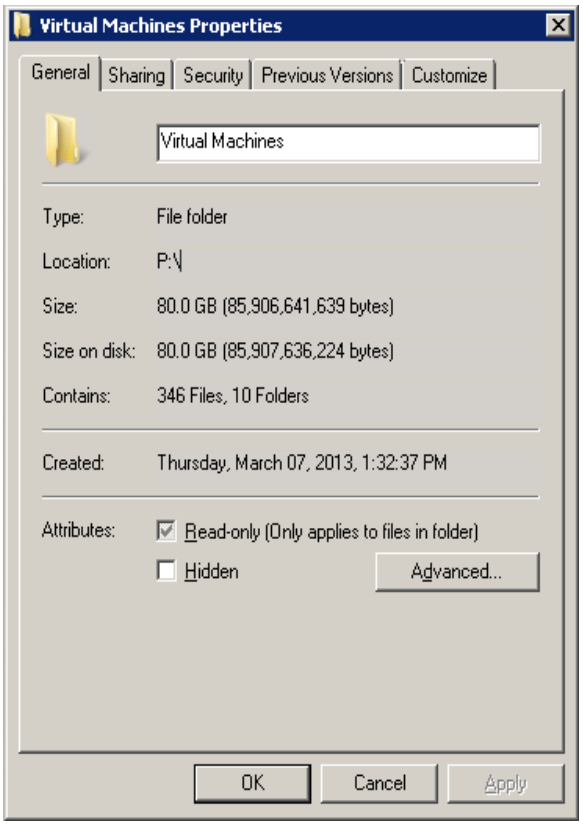


Figure 5 Uncompressed Virtual Machines Folder

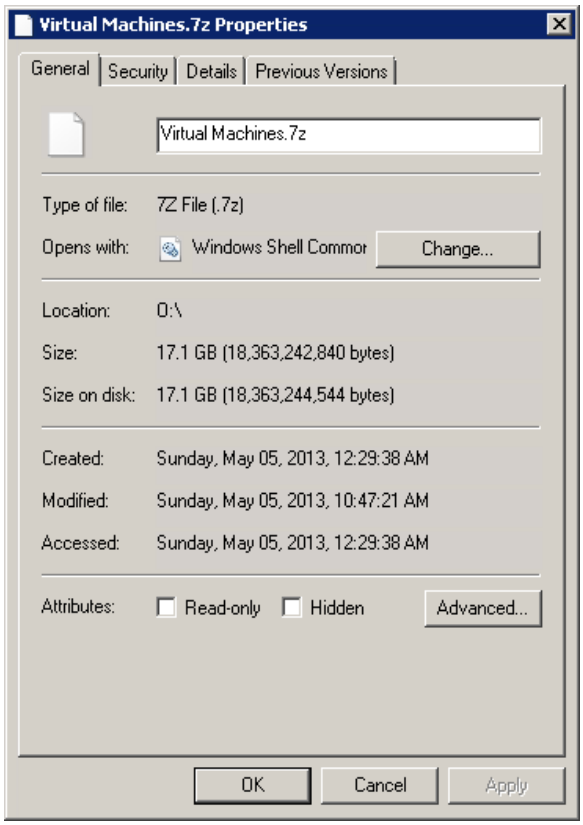


Figure 6 Compressed Virtual Machines Folder

Compressing the files enabled me to speed up the transfer process from the server on which the virtual machines were previously running to the virtual machine that I would use to perform the forensic analysis. Despite the compression, the transfer process took several hours.

Data Preservation

Once the archive was transferred to the forensic virtual machines, I proceeded to decompress the virtual machines folder archive using 7-Zip. After decompression, I re-ran HashMyFiles to ensure that no changes were made to the virtual machine files during transport, and found that the files were unchanged and unmodified as all of the hashes were identical to the hashes calculated prior to transfer to the forensic virtual machine:

Table 6 Hash Calculations after Transfer

Filename	MD5	SHA1	SHA-256	Full Path	Modified Time	Created Time	File Size
Windows 7-flat.vmdk	8800bcad1a173fd07a1b74f11c8545b9	81290ce989246c28d140092a46f60e1e91d1d89f	71d09c2280225235d18b30f5599ae37fef4d2f38a98499c615f05fc6632e2f11	F:\Virtual Machines\Windows 7\Windows 7-flat.vmdk	5/4/2013 3:59:42 PM	5/7/2013 9:12:47 AM	42949672960
Windows 8-flat.vmdk	752594eab4acf342891d7fe4421e4777	9ca91f650de285d2af8f863b1c2efeee7310ea34	3643019d5ed03d6ee4a245183e3897eb665a0d392dbf5504a4b51f346bdfefaa	F:\Virtual Machines\Windows 8\Windows 8-flat.vmdk	5/4/2013 3:59:25 PM	5/7/2013 9:51:52 AM	42949672960

Once I completed my forensic analysis, I also re-ran HashMyFiles to ensure that no changes were made to the virtual machine files during my analysis, and found that the files were unchanged and unmodified as all of the hashes were identical to the hashes calculated prior to and after transfer to the forensic virtual machine:

Table 7 Hash Calculations after Forensic Analysis

Filename	MD5	SHA1	SHA-256	Full Path	Modified Time	Created Time	File Size
Windows 7-flat.vmdk	8800bcad1a173fd07a1b74f11c8545b9	81290ce989246c28d140092a46f60e1e91d1d89f	71d09c2280225235d18b30f5599ae37fef4d2f38a98499c615f05fc6632e2f11	F:\Virtual Machines\Windows 7\Windows 7-flat.vmdk	5/4/2013 3:59:42 PM	5/7/2013 9:12:47 AM	42949672960
Windows 8-flat.vmdk	752594eab4acf342891d7fe4421e4777	9ca91f650de285d2af8f863b1c2efeee7310ea34	3643019d5ed03d6ee4a245183e3897eb665a0d392dbf5504a4b51f346bdfefaa	F:\Virtual Machines\Windows 8\Windows 8-flat.vmdk	5/4/2013 3:59:25 PM	5/7/2013 9:51:52 AM	42949672960

By calculating multiple hashes of the Windows 7 and Windows 8 virtual machine disk files and comparing them throughout the forensic process, I was able to insure that the data was preserved. This was extremely important; without data preservation, all of my findings would not be forensically sound as the original files would have changed.

Data Analysis

After I transferred the significant virtual machine files and calculated their hashes, I then proceeded to perform my data analysis. I used the commonly used forensic tools of AccessData Forensic Toolkit, AccessData Registry Viewer, and Guidance Software EnCase Forensic along with Magnet Forensic Internet Evidence Finder to uncover the previously generated user data just as a forensic investigator would.

Using each of the tools mentioned above, I proceeded to explore the file structure of the virtual machines looking for forensic artifacts. Because the artifacts I was searching for were known to me through the data generation process, locating artifacts was relatively easy. I searched for artifacts related to file activities, web browsing, social media, email, and the registry that would be useful to a forensic investigator were they to investigate both virtual machines for common user activities. The findings of my data analysis can be found in the Reporting section.

Reporting

For each virtual machine, I created a forensic report that follows a basic template of information that a forensic investigator might be interested in. The categories that I included are as follows:

- File Creation/Deletion Artifacts
- Web Browsing Artifacts
    - Internet Explorer/Internet Explorer App
    - Firefox
    - Chrome
- Social Media Artifacts
    - Facebook Activity
    - Twitter Activity
    - Facebook URLs
    - IEF Timeline
- Email Artifacts
- Registry Artifacts
    - Windows User Hive
    - Windows System Hive
    - Windows Software Hive
    - Security Account Manager (SAM)

While this is not an exhaustive list of everything a forensic investigator might be interested in, it is a good list for the activities that I performed during the data generation process. The complete forensic reports for Windows 7 and Windows 8 can be found in Appendix B and Appendix C respectively.

Results and Comparison

In this section, I detail the forensic similarities and differences for Windows 7 and Windows 8; uncovered through my forensic examination and reporting. For each of the categories listed in the Reporting section above, I have compared the results from the Windows 7 Forensic Report and Windows 8 Forensic Report.

File Creation and Deletion Artifacts

Similarities:

Using FTK, I was easily able to locate the files that I had created within the Windows7 or Windows8 user directories within C:\Users\. For both Windows 7 and Windows 8 I found the text files that I had created each day I generated data, as well as the text files I created for use as attachments with emails.

Additionally, I found that I was able to recover deleted files from Windows 7 and from Windows 8 even after the recycle bin was emptied. Using the recover folders task within the evidence processor for EnCase, I was able to uncover files for both operating systems quite easily, though I did need to manually search through the recovered folders and files. The recover folders task searches through the unallocated clusters of the file system as well as the Master File Table to locate previously deleted files and folders. Once the evidence processor completed processing the separate evidence files for Windows 7 and Windows 8, I was able to search the recovered files folders for the files that I had deleted during the data generation process. I simply had to open the Recovered Folders virtual folder within the root of the partition of the forensic image.

Differences:

There were really no significant differences in regards to file creation/deletion artifacts between Windows 7 and Windows 8. It took me longer to find the previously created and then deleted files for Windows 8 than it did for Windows 7, but I was still able to find them through the same process, so this really shouldn't be considered a difference. Ultimately, I was eventually able to use EnCase and FTK to recover files that I had created as well as files that I had deleted for both Windows 7 and Windows 8.

Web Browsing Artifacts

Similarities:

For Internet Explorer and the Internet Explorer App, EnCase was able to uncover artifacts including the web history and bookmarks of the web browsers that were created during the data generation process.

For Firefox, the EnCase Records Processor was able to recover the same types of information within Windows 7 as it was able to recover in Windows 8. For both operating systems, EnCase found web history, favorites, cached files and pictures, and even login data from Facebook and Twitter.

As was the case with Firefox, the EnCase Records Processor was able to recover the same types of information for the Chrome web browser within Windows 7 as it was able to recover in Windows 8. For both operating systems, EnCase found web history, top sites, cached files and pictures, as well as login data from Facebook and Twitter.

Differences:

For Windows 7, I was able to recover some of Internet Explorer's cached data using EnCase's Records Processor including pictures that appeared on websites visited during the data generation process and temporary internet files. That was not the case with Windows 8 and Internet Explorer as well as the Internet Explorer App. EnCase was unable to recover any cached files, images, or temporary internet files.

There were virtually no differences between Firefox and Chrome on Windows 7 and Firefox and Chrome on Windows 8. I suspect this to be the case because both Firefox and Chrome are supported for Windows 7 and Windows 8 and likely have nearly identical code for the executable files. The argument could be made that there should be an identical number of web browsing artifacts for both Windows 7 and Windows 8; that is not the case. But really, having exactly the same number of artifacts is unlikely to occur anyway.

Social Media Artifacts

Similarities:

Using FTK, I was able to find evidence of social media use through the Live Search Feature. Both virtual machines found the keywords "facebook" and "twitter" within allocated and unallocated space.

The real significant findings came from Magnet Forensic's Internet Evidence Finder (IEF). While IEF did not find all of the actions I performed over the course of generating data, it was able to find a majority of the social media activities. I was able to uncover activity from Facebook including comments from Firefox, Internet Explorer, and Chrome, and even the People App for Windows 8. I was also able to uncover activity from Twitter including tweets and

retweets. One of the interesting things IEF found for both Windows 7 and Windows 8 was a number of Facebook URLs from carved history or recorded browser activity. There were a number of potential activities that were found but they were the same for both operating systems. Finally, IEF was able to build a timeline of social media activity for the two virtual machines. The timelines are nearly identical with a few minor exceptions.

Differences:

There was very little difference in regards to recovering social media artifacts from Windows 7 and Windows 8. Technically you could argue that there should be an identical number of social media artifacts for both Windows 7 and Windows 8; that is not the case. Still, things were essentially identical. I believe this to be the case because most social media activities were performed through web browsers.

Email Artifacts

Similarities:

Using FTK, I was able to recover emails for the Gmail and Live email accounts for both Windows 7 and Windows 8. Using FTK, and its ability to locate email items, I was able to recover the emails that I sent and received. I was also able to recover the emails that had attachments included with them for both Windows 7 and Windows 8, but was unable to view the attachments themselves through the content viewer. I was able to see the information pertaining to the attachment but not view them, even though I was able to locate each of the files through a keyword search using both EnCase and FTK for Windows 7 and Windows 8.

Differences:

The primary difference that exists pertains to the number of emails that FTK discovered. While the number of emails that were received by the Gmail and Live accounts are different, this is insignificant and to be expected. However, the number of emails that were listed as sent by the Gmail and Live accounts for Windows 7 and Windows 8 should be identical; yet they are not. According to FTK, the Gmail accounts for Windows 7 and Windows 8 sent a total of 35 and 23 emails, respectively. According to FTK, the Live accounts for Windows 7 and Windows 8 sent a total of 27 and 11 emails, respectively.

The same thing occurred when I examined the Forwarded Emails and Email Replies for Windows 7 and Windows 8. The number of emails that FTK uncovered for the Windows7 Live and Gmail accounts on the Windows 7 virtual machine was more than those uncovered for the Windows8 Live and Gmail accounts on the Windows 8 virtual machine; despite the fact that they should have been identical as I forwarded/replied to the same number of emails during the data generation process for Windows 7 as I did for Windows 8.

Another significant difference between Windows 7 and Windows 8 email forensics is related to email attachments. The FTK email tool was unable to locate any email attachments for the Windows7 virtual machine while same tool was able to locate 36 total attachments for the Windows 8 virtual machine. This is a forensic difference between Windows 7 and Windows 8. It is unclear as to why FTK was unable to locate any email attachments for the Windows 7 virtual machine.

Registry Artifacts

Similarities:

Within the User Hive (NTUSER.dat), I explored the NTUSER.DAT\Software\ Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ OpenSavePIDIMRU registry key. This key existed for both Windows 7 and Windows 8 and provided the listing of files that had been opened or saved recently. I also explored the NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\ComDlg32\ LastVisitedMRUregistry key. This key existed for both Windows 7 and Windows 8 and provided the listing of applications that were recently used to open or save the files listed in the OpenSavePIDIMRU registry key. In addition, the NTUSER.DAT\Software\ Microsoft\Windows\Current Version\Explorer\RecentDocs existed for both Windows 7 and Windows 8 and it showed a listing of files and folders that were recently opened.

Within the System Hive (SYSTEM.dat), I explored the SYSTEM.DAT\ControlSet002\ Control\TimeZoneInformation registry key. This key existed for both Windows 7 and Windows 8 and provided identical information related to the time zone of the corresponding virtual machine.

With the Software Hive (SOFTWARE.dat), I explored the SOFTWARE.DAT\Microsoft\ WindowsNT\CurrentVersion\NetworkList\Signatures\Unmanaged registry key. This key existed

for both Windows 7 and Windows 8 and provided information related to the network history of the corresponding virtual machine.

For the SAM Hive (SAM.dat), I took a look at the registry key SAM.dat\Domains\ Accounts\Users. This key existed for both Windows 7 and Windows 8 and provided information relating to the user information of the corresponding virtual machine.

Differences:

Within the User Hive, the NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\ Explorer\ComDlg32\OpenSavePIDIMRU registry key differed in the number of items that it stored. For Windows 7, the key held a total of 8 items. For Windows 8, the key held a total of 20 items.

Related Works Findings

As previously mentioned in the literature review section, there are very few papers and articles that touch on the subject of Windows 8 Forensics. Still, there has been some research conducted in this area. Using this information in conjunction with my findings, we can more completely understand how Windows 8 differs forensically from Windows 7.

While Amanda C. F. Thomson's "Windows 8 Forensic Guide" is based upon the Consumer Preview version of Windows 8, whereas my research is based upon the released to manufacturing general availability version, it is really the best source of information for discovering additional forensic differences. [10] In addition to the many findings that my research details, the author was able to uncover the location of many applications that would be of forensic importance within the %Root%\Users\%User%\AppData\Local\ folder that may not exist in Windows 7 or differ from Windows 7:

Table 8 Thomson's Local Folder Differences

Application	Location	Purpose
Metro Apps	Microsoft\Windows\Application Shortcuts	Apps that are displayed on the Metro interface
IE 10 Websites Visited	Microsoft\InternetExplorer\Recovery\ Immersive\Active	Websites user visited while browsing with IE10.
	Microsoft\InternetExplorer\Recovery\ Immersive\Last Active	
Journal Notes	Microsoft\Journal\Cache\msnb.dat	Contains a history of journal notes created by user and their location.
User Added IE 10 Favorites	Microsoft\Windows\RoamingTiles	Websites the user has pinned to their favorites.
Desktop	Microsoft\Windows\WinX	Contains link files for applications such as Device Manager, Command Prompt, and Run.
Metro App Web Cache	Packages\%MetroAppName%\AC\INetCache	Contains web cache specific to Metro App.
Metro App Cookies	Packages\%MetroAppName%\AC\INetCookies	Contains cookie files specific to Metro App. Data is contained in a text file.
Metro App Web History	Packages\%MetroAppName%\AC\INetHistory	Contains Internet history files specific to Metro App and the format of the data is consistent with previous versions.
Metro Settings	Packages\%MetroAppName%\AC\LocalState	Contains settings specific to Metro App and can be viewed in plain text.

It should be noted that some of the information found by Thomson may no longer be accurate given that these findings are based upon Windows 8 Consumer Preview. In fact, a major change between the Consumer Preview and the General Availability release include the renaming of the Communication App to the People App. Much of the "Windows 8 Forensic Guide" lists that the location of forensic artifacts exists in the same location they did in Windows 7 including the Roaming Folder (%Root%\Users\%User%\AppData\Roaming\), and much of the Windows Registry with the exception of a few registry keys:

Table 9 Thomson's Windows 8 Registry Differences

Registry Hive	Data Stored	Registry Key Location
NTUSER.DAT	Typed URL Time	Software\Microsoft\Internet Explorer\TypedURLsTime
SAM.DAT	Internet User Name (Windows Live Account)	Domains\Account\Users\InternetUserName
SAM.DAT	User's Tile:	Domains\Account\Users\UserTile
SYSTEM.DAT	Sensors & Location Devices	CurrentControlSet\Enum\SWD\SensorsAndLocation- Enum\HardwareID
SOFTWARE.DAT	Metro Apps Installed on System	Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\ Applications
SOFTWARE.DAT	User Account Installed Metro Apps	Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\%SID%

In most cases, Thomson found that the Windows 8 registry behaved in the same way and was nearly identical structurally to the Windows 7 registry. Thomson's findings with the registry regarding the differences between Windows 7 and Windows 8 are consistent with my research.

In his blog posts and YouTube videos, "Windows 8 Forensics", Ethan Fleisher determined that there is little to no forensic difference between Windows 7 and Windows 8. [11] The author did uncovered that Internet cookies and history files are stored in different locations from the previous version of Windows.

Table 10 Fleisher's Internet Cookies and History File Location Differences

Cookies	<root>\users\<username>\appdata\roaming\ microsoft\windows\cookies\	<root>\users\<username>\appdata\roaming\ microsoft\windows\cookies\low
Temporary Internet Files	<root>\users\<username>\appdata\local\ microsoft\microsoft\windows\history contained in index.dat	<root>\users\<username>\appdata\local\ microsoft\microsoft\windows\history contained in container.dat

While these are certainly differences between Windows7 and Windows 8, they are hardly groundbreaking. Fleisher's findings support what I found through the use of EnCase and FTK that Cookies and Temporary Internet Files still exist within Windows 8 and aren't especially difficult to locate.

In his presentation, "Windows 8 A Forensic First Look", Josh Brunty points out a major difference between Windows 7 and Windows 8; each immersive application has its own registry file and own Internet artifacts (Cache, Cookies, History). This is consistent with Thomson's findings previously mentioned as well as my own research.

In his blog Random Thoughts of Forensics, Ken Johnson confirms some of the findings previously mentioned but also points out that once Windows 8 File History Service is enabled, numerous artifacts are created that would be of use to a forensic investigator. [15] Johnson's blog posts also explore the refresh and recovery options of Windows 8. He found that even if a computer is reset or recovered, some data is still left behind in $SysReset and Windows.old directories on the hard drive:

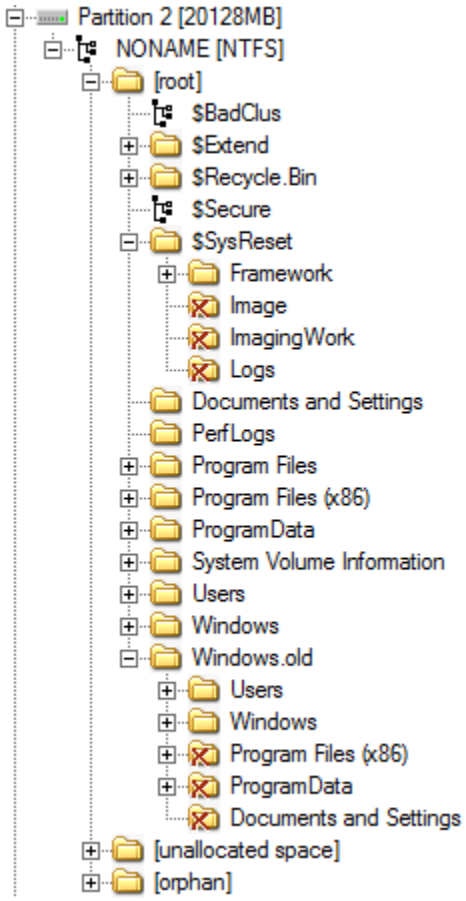


Figure 7 Johnson's Refresh and Recovery Differences

I was unable to explore the refresh and recovery options, primarily due to the fact that I did not want to compromise my forensic images, but this is a difference with Windows 8, even if those options were unavailable in the same capacity for Windows 7.

Future Work

While the research that I did conduct took a great deal of time to develop, implement, document, and finally report on, there are still opportunities for additional research to be conducted. For example, it might be interesting to do a comparison of the file structure of a plain, vanilla, installation of Windows 7 and Windows 8. This would highlight many of the differences that other researchers and myself have uncovered, but would also likely aid in the discovery of additional differences. It also might be useful to do something similar for the registry hives of Windows 7 and Windows 8; my research points out a few of the differences, but there are likely to be many more. As mentioned earlier, it would be worthwhile to explore the process through

which Windows 8 deleted files and compare that with Windows 7. Finally, additional work could be conducted with the latest update to the operating system: Windows 8.1. I would suspect that things would be very similar to Windows 8, but without research to confirm that is the case it is unknown if they are forensically similar.

Conclusion

Windows 7 and Windows 8 are distinct and separate operating systems. However, they are both Microsoft operating systems, and while they may have noteworthy differences, at their core they behave in a similar fashion. Visually, Windows 8 vastly differs from Windows 7; the new modern interface drastically changes how users interact with the system. The introduction of "apps" in Windows 8 is also a stark difference from Windows 7. Despite these differences, the Windows Registry structure remains largely intact and similar. The file structure of Windows 8 is similar to that of Windows 7, with the exception to the addition of modern application files and folders. Even though Windows 8 was intended to be a complete redesign, there are many parts of previous Microsoft Windows operating systems that are leveraged. Because of this, the forensic difference between Windows 7 and Windows 8 is minimal.

Appendices

Appendix A: User Data Log

04/21/2013

Windows 7 around 3:20PM

Activated Windows 7

Installed Windows Essentials 2012: Mail and SkyDrive

Installed Google Chrome

Install Mozilla Firefox

In each browser, set favorites for Facebook, Twitter, Email Accounts, Wikipedia Featured Article, RIT News

Setup Windows Live Mail 2012 with Email Accounts: PeterWilson.Win7@gmail.com and PeterWilson.Win7@live.com

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Reginald_Heber

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49953&source=enewsletter and http://www.rit.edu/news/story.php?id=49951&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Logged In, told browsers to remember password

Using IE, Firefox, and Chrome Browsed to Twitter, Logged In, told browsers to remember username and password

Using Windows Live Mail 2012, added contacts for all email accounts

Using Windows Live Mail 2012, sent email to other 3 accounts from the Live Account

Using IE Shared IST at RIT Post on Facebook

Using Firefox Tweeted Daily Tweet

Using Chrome Posted Daily Post on Facebook

Windows 8 around 4:05PM

Connected Window 8 to Live Account PeterWilson.Win8@live.com

Installed Google Chrome

Install Mozilla Firefox

In each browser, set favorites for Facebook, Twitter, Email Accounts, Wikipedia Featured Article, RIT News

Setup Mail App with Email Accounts: PeterWilson.Win7@gmail.com and PeterWilson.Win7@live.com

Using People Application, added contacts for all email accounts

Using People Application, connected to Facebook

Using People Application, connected to Twitter

Using Mail App, sent email to other 3 accounts from the Live Account

Using IE App, IE Desktop, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Reginald_Heber

Using IE App, IE Desktop, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49953&source=enewsletter and http://www.rit.edu/news/story.php?id=49951&source=enewsletter

Using IE App, IE Desktop, Firefox, and Chrome Browsed to Twitter, Logged In, told browsers to remember username and password

Using IE Desktop Shared IST at RIT Post on Facebook

Using Firefox Tweeted Daily Tweet

Using Chrome Posted Daily Post on Facebook

Broswed through What's new in the People app

Viewed unread notification in the People app

Using the Weather app, allowed location services, added home/favorite location Rochester, NY

04/23/2013

Windows 7 around 9:30PM

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Alcohol_laws_of_New_Jersey

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49963&source=enewsletter and http://www.rit.edu/news/story.php?id=49964&source=enewsletter and http://www.rit.edu/news/story.php?id=49962&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account

Using Chrome Shared Rochester Institute of Technology's Photo on Facebook

Using IE Tweeted Daily Tweet

Using IE Retweeted @RITNEWS Tweet

Using Firefox Posted Daily Post on Facebook

Downloaded File mirrors.rit.edu/centos/6.4/isos/i386/CentOS-6.4-i386-netinstall.iso to C:\Users\Windows7\Downloads folder using IE

Created File C:\Users\Windows8\Documents\04232013daily.txt

Windows 8 around 10:30pm

Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Alcohol_laws_of_New_Jersey

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49953&source=enewsletter and http://www.rit.edu/news/story.php?id=49951&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Mail App, sent email to other 3 accounts from the Gmail Account

Using People App Tweeted Daily Tweet

Using People App Posted Daily Post on Facebook

Using People App Retweeted @RITNEWS Tweet

Downloaded File mirrors.rit.edu/centos/6.4/isos/i386/CentOS-6.4-i386-netinstall.iso to Downloads folder using IE App

Created File C:\Users\Windows8\Documents\04232013daily.txt

04/24/2013

Windows 7 around 9:10PM

Created File C:\Users\Windows7\Documents\04242013deleted.txt

Created File C:\Users\Windows7\Documents\04242013attachment.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Live Account with Attached File 04232013attachment.txt

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Military_history_of_Australia_during_World_War_II

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49965&source=enewsletter and http://www.rit.edu/news/story.php?id=49958&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Downloaded File http://mirrors.rit.edu/centos/6.4/isos/i386/README.txt to C:\Users\Windows7\Downloads folder using Firefox

Using Firefox Shared IST at RIT's Post on Facebook about being a TA

Using Chrome Tweeted Daily Tweet

Using Chrome Retweeted @RITsports Tweet

Using IE Posted Daily Post on Facebook

Deleted Chrome and Firefox Shortcuts from Desktop

Delete File C:\Users\Windows7\Documents\04242013deleted.txt at 9:26PM

Checked for Updates, No important updates to install

Windows 8 around 9:30PM

Created File C:\Users\Windows7\Documents\04242013deleted.txt

Created File C:\Users\Windows7\Documents\04242013attachment.txt

Using Mail App, sent email to other 3 accounts from the Live Account with Attached File 04232013attachment.txt

Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Military_history_of_Australia_during_World_War_II

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49965&source=enewsletter and http://www.rit.edu/news/story.php?id=49958&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Downloaded File http://mirrors.rit.edu/centos/6.4/isos/i386/README.txt to C:\Users\Windows8\Downloads folder using Firefox

Using Firefox Shared IST at RIT's Post on Facebook about being a TA

Using Chrome Tweeted Daily Tweet

Using Chrome Retweeted @RITsports Tweet

Using IE App Posted Daily Post on Facebook

Deleted Chrome and Firefox Shortcuts from Desktop

Delete File C:\Users\Windows8\Documents\04242013deleted.txt at 9:42PM

Checked for Updates, Installed 1 Important Update

Using Weather App looked at weather for Rochester, NY and Seattle, WA

Using Map App, Set home as Rochester Institute of Technology 117 Lomb Memorial Drive, Rochester, NY

Using Map App, got Directions from Home (RIT) to Seattle, WA by Driving, looked at 3 different routes

04/25/2013

Windows 7 around 9:50PM

Created File C:\Users\Windows7\Documents\04252013daily.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Franco-Mongol_alliance

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49671&source=enewsletter and http://www.rit.edu/news/story.php?id=49968&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE Shared Rochester Institute of Technology's Photo on Facebook about RIT/NTID

Performing Arts

Using IE Reply to Daily Tweet

Using Firefox Tweeted Daily Tweet

Using Firefox Retweeted @ForensicFocus Tweet

Using Chrome Posted Daily Post on Facebook

Using Chrome Commented on Daily Facebook Post

Downloaded File http://mirrors.rit.edu/openoffice/packages/14/OOo_3.3.0_Win_x86_install_om.exe to C:\Users\Windows7\Downloads folder using Chrome

Deleted File C:\Users\Windows7\Downloads\CentOS-6.4-i386-netinstall.iso at 10:04PM

Using Windows Live Mail 2012 Reply to the Daily Email using Live Account to PeterWilson.Win7@gmail.com

Using Windows Live Mail 2012 Forward the Daily Email using Live Account to PeterWilson.Win7@gmail.com

Checked for Updates, No important updates to install

Viewed About Information for Facebook, Set all Email Addresses to be viewable by Friends

Windows 8 around 10:12PM

Created File C:\Users\Windows8\Documents\04252013daily.txt

Using Mail App, sent email to other 3 accounts from the Gmail Account

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Franco-Mongol_alliance

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49671&source=enewsletter and http://www.rit.edu/news/story.php?id=49968&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE App Shared Rochester Institute of Technology's Photo on Facebook about RIT/NTID Performing Arts

Using People App Reply to Daily Tweet

Using Firefox Tweeted Daily Tweet

Using Firefox Retweeted @ForensicFocus Tweet

Using Chrome Posted Daily Post on Facebook

Using Chrome Commented on Daily Facebook Post

Downloaded File http://mirrors.rit.edu/openoffice/packages/14/OOo_3.3.0_Win_x86_install_om.exe to C:\Users\Windows8\Downloads folder using Chrome

Deleted File C:\Users\Windows8\Downloads\CentOS-6.4-i386-netinstall.iso at 10:30PM

Using Mail App Reply to the Daily Email using Live Account to PeterWilson.Win8@gmail.com

Using Mail App Forward the Daily Email using Live Account to PeterWilson.Win8@gmail.com

Viewed About Information for Facebook, Set all Email Addresses to be viewable by Friends

Checked for Updates, installed 1 Important Update

Turned on Windows SmartScreen

04/26/2013

Windows 7 around 11:30AM

Created File C:\Users\Windows7\Documents\04262013daily.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Live Account

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Franco-Mongol_alliance

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49968&source=enewsletter and http://www.rit.edu/news/story.php?id=49972&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Chrome Shared http://www.rit.edu/news/story.php?id=49968&source=enewsletter through link on page on Facebook

Using Chrome Reply to Daily Tweet

Using IE Tweeted Daily Tweet

Using IE Retweeted @RIT_SportsZone Tweet

Using Firefox Posted Daily Post on Facebook

Using Firefox Like and Commented on Daily Facebook Post

Downloaded File http://mirrors.rit.edu/ubuntu-releases/13.04/ubuntu-13.04-server-i386.iso to C:\Users\Windows7\Downloads folder using IE

Using Windows Live Mail 2012 Reply to the Daily Email using Gmail Account to PeterWilson.Win7@live.com

Using Windows Live Mail 2012 Forward the Daily Email using Gmail Account to PeterWilson.Win7@live.com

Emptied the Recycle Bin at 12:00PM

Windows 8 around 11:50AM

Created File C:\Users\Windows8\Documents\04262013daily.txt

Using Mail App, sent email to other 3 accounts from the Live Account

Using IE App, IE , Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Franco-Mongol_alliance

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day:

http://www.rit.edu/news/story.php?id=49968&source=enewsletter and
http://www.rit.edu/news/story.php?id=49972&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Chrome Shared http://www.rit.edu/news/story.php?id=49968&source=enewsletter on Facebook through link on page

Using Chrome Reply to Daily Tweet

Using IE App Tweeted Daily Tweet

Using IE App Retweeted @RIT_SportsZone Tweet

Using Firefox Posted Daily Post on Facebook

Using Firefox Like and Commented on Daily Facebook Post

Downloaded File http://mirrors.rit.edu/ubuntu-releases/13.04/ubuntu-13.04-server-i386.iso to C:\Users\Windows8\Downloads folder using IE (Downloaded very slowly)

Using Mail App Reply to the Daily Email using Gmail Account to PeterWilson.Win8@live.com

Using Mail App Forward the Daily Email using Gmail Account to PeterWilson.Win8@live.com

Opened the People App and viewed unread notifications clicked on What's New Twitter and Facebook

Opened the Finance App Scrolled Through

Opened the Sports App Scrolled Through

Emptied the Recycle Bin at 12:30PM

04/28/2013

Windows 7 around 3:40PM

Created File C:\Users\Windows7\Documents\04282013daily.txt

Create C:\Users\Windows7\Documents\04282013deleted.txt

Using IE downloaded RIT logo pictures to C:\Users\Windows7\Downloads

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account with two Pictures Attached

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/1923_FA_Cup_Final

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49972&source=enewsletter and
http://www.rit.edu/news/story.php?id=49974&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Firefox Shared IST at RIT's Post on Facebook

Using Firefox Reply to Daily Tweet

Using Chrome Tweeted Daily Tweet

Using Chrome Retweeted @RITsports Tweet

Using IE Posted Daily Post on Facebook

Using IE Like and Commented on Daily Facebook Post

Deleted C:\Users\Windows7\Documents\04282013deleted.txt at 4:04PM

Windows 8 around 4:08

Created File C:\Users\Windows8\Documents\04282013daily.txt

Create C:\Users\Windows8\Documents\04282013deleted.txt

Using IE downloaded RIT logo pictures to C:\Users\Windows8\Downloads

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account with two Pictures Attached

Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/1923_FA_Cup_Final

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49972&source=enewsletter and http://www.rit.edu/news/story.php?id=49974&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE App Shared IST at RIT's Post on Facebook

Using People App Reply to Daily Tweet

Using People App Tweeted Daily Tweet

Using People App Retweeted @RITsports Tweet

Using People App Posted Daily Post on Facebook

Using People App Like and Commented on Daily Facebook Post

Looked at Weather using the Weather App

Deleted C:\Users\Windows7\Documents\04282013deleted.txt at 4:22PM

05/01/2013

Windows 7 around 11:15AM

Created File C:\Users\Windows7\Documents\05012013daily.txt

Create C:\Users\Windows7\Documents\05012013deleted.txt

Created File C:\Users\Windows7\Documents\05012013attachment.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Live Account with two Pictures and 05012013attatchment.txt attached

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/If_Day

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day:

http://www.rit.edu/news/story.php?id=49956&source=enewsletter and
http://www.rit.edu/news/story.php?id=49976&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE Shared rochester Institute of Technology's Photo on Facebook

Using IE Reply to Daily Tweet

Using Firefox Tweeted Daily Tweet

Using Firefox Retweeted @RITsports Tweet

Using Chrome Posted Daily Post on Facebook

Using Chrome Like and Commented on Daily Facebook Post

Downloaded File http://mirrors.rit.edu/fedora/linux/releases/18/Live/i386/Fedora-18-i686-Live-Desktop.iso to Downloads folder using IE (Downloaded very Slowly)

Using Windows Live Mail 2012, Reply to the Daily Email using Live Account to PeterWilson.Win7@gmail.com

Using Windows Live Mail 2012, Forward the Daily Email using Live Account to PeterWilson.Win7@gmail.com

Checked for Updates, no important updates

Windows 8 around 11:40PM

Created File C:\Users\Windows8\Documents\05012013daily.txt

Create C:\Users\Windows8\Documents\05012013deleted.txt

Created File C:\Users\Windows8\Documents\05012013attachment.txt

Using Mail App, sent email to other 3 accounts from the Live Account with two Pictures and 05012013attatchment.txt attached

Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/If_Day

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49956&source=enewsletter and
http://www.rit.edu/news/story.php?id=49976&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE App Shared Rochester Institute of Technology's Photo on Facebook

Using IE Reply to Daily Tweet

Using Firefox Tweeted Daily Tweet

Using IE APP Retweeted @RITsports Tweet

Using Chrome Posted Daily Post on Facebook

Using IE App Like and Commented on Daily Facebook Post

Downloaded File http://mirrors.rit.edu/fedora/linux/releases/18/Live/i386/Fedora-18-i686-Live-

Desktop.iso to Downloads folder using IE App (Downloaded very Slowly around 3 hours)

Opened the People App and viewed unread notifications clicked on What's New Twitter and Facebook

Opened the Finance App Scrolled Through, Looked Up MSFT ticker added it to watchlist

Opened the Sports App Scrolled Through

Using Map App, got Driving Directions from Home (RIT) to Los Angeles, CA by Driving, looked at different routes

Using Mail App Reply to the Daily Email using Live Account to PeterWilson.Win8@gmail.com

Using Mail App Forward the Daily Email using Live Account to PeterWilson.Win8@gmail.com

Checked for Updates

05/02/2013

Windows 7 around 10:45AM

Deleted C:\Users\Windows7\Documents\05012013deleted.txt at 10:46AM

Created File C:\Users\Windows7\Documents\0502013daily.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/United_States_v._The_Progressive

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49981&source=enewsletter and http://www.rit.edu/news/story.php?id=49984&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Chrome Shared Rochester Institute of Technology's Photo on Facebook

Using Chrome Reply to Daily Tweet

Using IE Tweeted Daily Tweet

Using IE Retweeted @RITNEWS Tweet

Using Firefox Posted Daily Post on Facebook

Using Firefox Like and Commented on Daily Facebook Post

Windows 8 around 11:25AM

Deleted C:\Users\Windows8\Documents\05012013deleted.txt at 11:26AM

Created File C:\Users\Windows8\Documents\0502013daily.txt

Using Mail App, sent email to other 3 accounts from the Gmail account

Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/United_States_v._The_Progressive

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49981&source=enewsletter and

http://www.rit.edu/news/story.php?id=49984&source=enewsletter

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Chrome Shared Rochester Institute of Technology's Photo on Facebook

Using Chrome Reply to Daily Tweet

Using IE Tweeted Daily Tweet

Using IE Retweeted @RITNEWS Tweet

Using Firefox Posted Daily Post on Facebook

Using Firefox Like and Commented on Daily Facebook Post

05/03/2013

Windows 7 around 4:30PM

Created File C:\Users\Windows7\Documents\0503013daily.txt

Create C:\Users\Windows7\Documents\05032013deleted.txt

Created File C:\Users\Windows7\Documents\05032013attachment.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Live Account with Attachment

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Mother_India

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49992&source=enewsletter and http://www.rit.edu/news/story.php?id=49993&source=enewsletter and http://www.rit.edu/news/story.php?id=49957&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IIE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using Chrome Tweeted Daily Tweet

Using Chrome Retweeted @RITSports Tweet

Using IE Posted Daily Post on Facebook

Using IE Like and Commented on Daily Facebook Post

Using Firefox Shared Rochester Institute of Technology's Photo on Facebook

Using Firefox Reply to Daily Tweet

Downloaded File http://mirrors.rit.edu/knoppix/KNOPPIX_V7.0.5bootonly-2012-12-21-EN.iso to Downloads folder using Chrome

Using Windows Live Mail 2012, Reply to the Daily Email using Live Account to PeterWilson.Win7@live.com

Using Windows Live Mail 2012, Forward the Daily Email using Live Account to PeterWilson.Win7@live.com

Deleted File C:\Users\Windows8\Documents\05032013deleted.txt at 4:50PM

Deleted File C:\Users\Windows8\Downloads\README.txt at 4:50PM

Checked for Updates, None to install

Windows 8 around 4:55PM

Created File C:\Users\Windows8\Documents\0503013daily.txt

Create C:\Users\Windows8\Documents\05032013deleted.txt

Created File C:\Users\Windows8\Documents\05032013attachment.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Live Account with Attachment

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/Mother_India

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49992&source=enewsletter and http://www.rit.edu/news/story.php?id=49993&source=enewsletter and http://www.rit.edu/news/story.php?id=49957&source=enewsletter

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using People App Tweeted Daily Tweet

Using People App Retweeted @RITSports Tweet

Using People App Posted Daily Post on Facebook

Using People App Like and Commented on Daily Facebook Post

Using Firefox Shared Rochester Institute of Technology's Photo on Facebook

Using People App Reply to Daily Tweet

Downloaded File http://mirrors.rit.edu/knoppix/KNOPPIX_V7.0.5bootonly-2012-12-21-EN.iso to Downloads folder using Chrome

Using Mail App, Reply to the Daily Email using Live Account to PeterWilson.Win7@live.com

Using Mail App, Forward the Daily Email using Live Account to PeterWilson.Win7@live.com

Deleted File C:\Users\Windows8\Documents\05032013deleted.txt at 7:26PM

Deleted File C:\Users\Windows8\Downloads\README.txt at 7:26PM

Checked for Updates, One important update to install

05/04/2013

Windows 7 around 3:31PM

Created File C:\Users\Windows7\Documents\0504013daily.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account

Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/George_Harrison

Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49994&source=enewsletter and http://www.rit.edu/imagine/

Using IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE Shared Rochester Institute of Technology's Photo on Facebook

Using IE Reply to Daily Tweet

Using Firefox Tweeted Daily Tweet

Using Firefox Retweeted @RITNEWS Tweet

Using Chrome Posted Daily Post on Facebook

Using Chrome Like and Commented on Daily Facebook Post

Deleted File OOo_3.3.0_Win_x86_install_om.exe from Downloads folder at 3:34PM

Emptied Recycle Bin at 3:45PM

Checked for updates, no important updates to install

Shutdown system at 3:59PM

Windows 8 around 3:45PM

Created File C:\Users\Windows8\Documents\0504013daily.txt

Using Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account

Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article: http://en.wikipedia.org/wiki/George_Harrison

Using IE App, IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day: http://www.rit.edu/news/story.php?id=49994&source=enewsletter and http://www.rit.edu/imagine/

Using IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In

Using IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In

Using IE Shared Rochester Institute of Technology's Photo on Facebook

Using IE App Reply to Daily Tweet

Using Firefox Tweeted Daily Tweet

Using Firefox Retweeted @RITNEWS Tweet

Using Chrome Posted Daily Post on Facebook

Using Chrome Like and Commented on Daily Facebook Post

Deleted File OOo_3.3.0_Win_x86_install_om.exe from Downloads folder at 3:46PM

Emptied Recycle Bin at 3:55PM

Checked for updates, 1 important update to install

Shutdown system at 3:58PM

Appendix B: Windows 7 Forensic Report

Windows 7 Forensic Report

05/28/2013

Introduction

This document serves as a detailed report of the forensic findings made while examining the Windows 7 virtual machine. Using both FTK and EnCase, I was able to uncover a majority of the user data that was generated. This report specifically looks at a number of different forensic artifacts including file creation/deletion, web browsing, social media, email and registry.

File Creation/Deletion

The first artifacts that I set out to discover were any artifacts pertaining to user file creation or deletion. In Windows 7, the majority of user files are stored within the C:\Users\ directory, which contains several subfolders for each created user. Given that the user I created is Windows7, I primarily looked in the Windows7 subfolder. This directory includes folders for Contacts, Desktop, Downloads, Favorites, Links, Documents, Music, Pictures, Videos, and several other folders.

While exploring the folders within the Windows7 user directory I was able to uncover several relevant artifacts. First, I was able to easily find many of the daily and attachment files that I created using FTK, though it is interesting to note that in some cases the files have a double extension:

Name	Ext	Created	Accessed	Modified	Path	P-Size	L-Size
$I30		3/7/2013 2:19:03 PM (2...	5/4/2013 3:34:38 PM (2...	5/4/2013 3:34:38 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/$I30	4096 B	4096 B
04232013daily.txt.txt	txt	4/23/2013 9:55:14 PM (...	4/23/2013 9:55:14 PM (...	4/23/2013 9:55:35 PM (...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/04232013daily.txt.txt	53 B	53 B
04242013attachment.txt.txt	txt	4/24/2013 9:11:32 PM (...	4/24/2013 9:11:32 PM (...	4/24/2013 9:11:57 PM (...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/04242013attachment.txt.txt	57 B	57 B
04252013daily.txt	txt	4/25/2013 9:50:36 PM (...	4/25/2013 9:50:36 PM (...	4/25/2013 9:50:59 PM (...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/04252013daily.txt	53 B	53 B
04262013daily.txt	txt	4/26/2013 11:31:06 AM...	4/26/2013 11:31:06 AM...	4/26/2013 11:31:06 AM...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/04262013daily.txt	46 B	46 B
04282013daily.txt.txt	txt	4/28/2013 3:40:29 PM (...	4/28/2013 3:40:29 PM (...	4/28/2013 3:40:58 PM (...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/04282013daily.txt.txt	45 B	45 B
05012013attachment.txt.txt	txt	5/1/2013 11:17:49 AM (...	5/1/2013 11:17:49 AM (...	5/1/2013 11:18:15 AM ...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/05012013attachment.txt.txt	91 B	91 B
05012013daily.txt.txt	txt	5/1/2013 11:16:40 AM (...	5/1/2013 11:16:40 AM (...	5/1/2013 11:17:06 AM ...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/05012013daily.txt.txt	46 B	46 B
05022013daily.txt.txt	txt	5/2/2013 10:46:47 AM (...	5/2/2013 10:46:47 AM (...	5/2/2013 10:47:37 AM ...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/05022013daily.txt.txt	48 B	48 B
05032013attachment.txt.txt	txt	5/3/2013 4:32:59 PM (2...	5/3/2013 4:32:59 PM (2...	5/3/2013 4:33:25 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/05032013attachment.txt.txt	78 B	78 B
05032013daily.txt.txt	txt	5/3/2013 4:32:30 PM (2...	5/3/2013 4:32:30 PM (2...	5/3/2013 4:32:51 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/05032013daily.txt.txt	45 B	45 B
0504013daily.txt.txt	txt	5/4/2013 3:34:36 PM (2...	5/4/2013 3:34:36 PM (2...	5/4/2013 3:34:54 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/0504013daily.txt.txt	47 B	47 B
desktop.ini	ini	3/7/2013 2:20:16 PM (2...	3/7/2013 2:20:16 PM (2...	3/9/2013 12:36:31 AM ...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/desktop.ini	402 B	402 B
My Music		3/7/2013 2:19:03 PM (2...	3/7/2013 2:19:03 PM (2...	3/7/2013 2:19:03 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/My Music	120 B	120 B
My Pictures		3/7/2013 2:19:03 PM (2...	3/7/2013 2:19:03 PM (2...	3/7/2013 2:19:03 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/My Pictures	132 B	132 B
My Videos		3/7/2013 2:19:03 PM (2...	3/7/2013 2:19:03 PM (2...	3/7/2013 2:19:03 PM (2...	Windows 7-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows7/Documents/My Videos	124 B	124 B

Figure 8 Windows 7 Created Documents

When I viewed the contents of the files, they simply contained whatever text I had placed into them when I first created them during the data generation process:

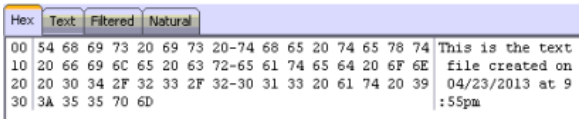


Figure 9 Windows 7 Created File

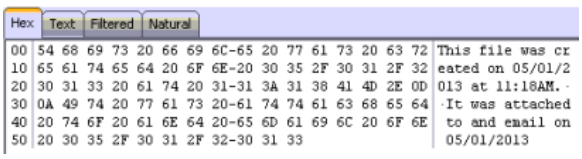
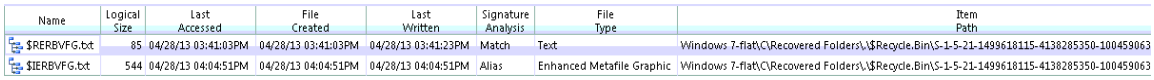


Figure 10 Windows 7 Created File

Uncovering the files that I deleted throughout the user data generation process was a bit more difficult. Using EnCase and its evidence processor, I was able to recover a few of the files that I had deleted. Unfortunately, the process was very arduous as I had to manually search through all of the recovered files and folders. I was able to find the file that I deleted on 04/28/2013 along with a reference to the original file location:



Name	Logical Size	Last Accessed	File Created	Last Written	Signature Analysis	File Type	Item Path
$RERBVFG.txt	85	04/28/13 03:41:03PM	04/28/13 03:41:03PM	04/28/13 03:41:23PM	Match	Text	Windows 7-flat\C\Recovered Folders\.\$Recycle.Bin\S-1-5-21-1499618115-4138285350-100459063
$IERBVFG.txt	544	04/28/13 04:04:51PM	04/28/13 04:04:51PM	04/28/13 04:04:51PM	Alias	Enhanced Metafile Graphic	Windows 7-flat\C\Recovered Folders\.\$Recycle.Bin\S-1-5-21-1499618115-4138285350-100459063

Figure 11 Windows 7 Recovered Deleted Files

The first file, $RERBVFG.txt had the following contents:

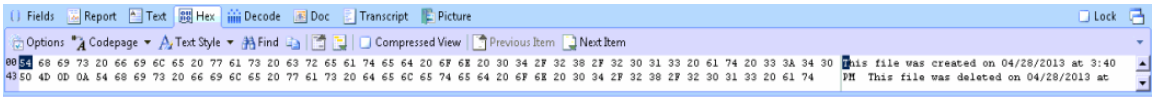


Figure 12 Recovered File $RERBVFG.txt

The second file, $IERBVFG.txt has the following contents:

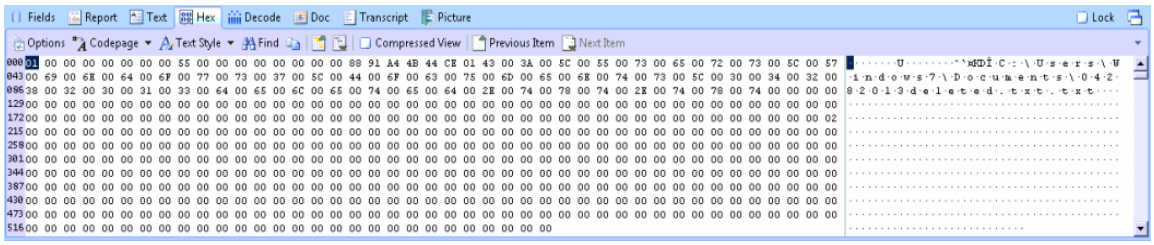


Figure 13 Recovered File $IERBVFG.txt

I attempted to run several other searches on both Lost Files and Recovered Folders and ended up with 218 results when I searched for the keyword “deleted”. When I sifted through the entire search results I was only able to find that the previously uncovered $RERBVFG.txt were files that I had deleted.

Web Browsing (Internet Explorer, Firefox, Chrome)

The second set of artifacts that I set out to uncover were web browsing artifacts. In the case of the Windows 7 virtual machine, Internet Explorer, Firefox and Chrome were the web browsers that I used to generate data. So, for each of the browsers I examined Internet history, downloads, favorites, and other temporary Internet files. Using EnCase and its records processor I was able to quickly uncover web browsing artifacts for all three browsers.

Internet Explorer

Uncovering information regarding web browsing with Internet Explorer was relatively simple. Using the EnCase records processor I was able to easily view the history, favorites, and cache. I the case of browsing history, EnCase examined the TypedURLs registry key within the Windows registry. This entry can be found within HKEY_CURRENT_User\Software\Microsoft\Internet Explorer\TypedURLs and thereby making it specific to the currently logged on user, in our case Windows 7. From the TypedURLs key, I was able to see a total of the twenty most recently viewed web pages, though it appears that they repeat after only ten:

Browser Type	Title	Last Modification Time	Url Name	Profile Name	Internet Artifact Type
Internet Explorer (Windows)	url1	05/01/13 11:30:55AM	http://mirrors.rit.edu/	Windows7	History\Typed URL
Internet Explorer (Windows)	url2	05/01/13 11:30:55AM	http://google.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url3	05/01/13 11:30:55AM	http://mirrors.rit.edu/centos/6.4/isos/i386/CentOS-6.4-i386-netinstall.iso	Windows7	History\Typed URL
Internet Explorer (Windows)	url4	05/01/13 11:30:55AM	http://live.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url5	05/01/13 11:30:55AM	http://gmail.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url6	05/01/13 11:30:55AM	http://twitter.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url7	05/01/13 11:30:55AM	http://facebook.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url8	05/01/13 11:30:55AM	http://www.rit.edu/news/nandedaily.php	Windows7	History\Typed URL
Internet Explorer (Windows)	url9	05/01/13 11:30:55AM	http://en.wikipedia.org/wiki/Main_Page	Windows7	History\Typed URL
Internet Explorer (Windows)	url10	05/01/13 11:30:55AM	http://go.microsoft.com/fwlink/?LinkId=69157	Windows7	History\Typed URL
Internet Explorer (Windows)	url1	05/01/13 11:30:55AM	http://mirrors.rit.edu/	Windows7	History\Typed URL
Internet Explorer (Windows)	url2	05/01/13 11:30:55AM	http://google.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url3	05/01/13 11:30:55AM	http://mirrors.rit.edu/centos/6.4/isos/i386/CentOS-6.4-i386-netinstall.iso	Windows7	History\Typed URL
Internet Explorer (Windows)	url4	05/01/13 11:30:55AM	http://live.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url5	05/01/13 11:30:55AM	http://gmail.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url6	05/01/13 11:30:55AM	http://twitter.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url7	05/01/13 11:30:55AM	http://facebook.com/	Windows7	History\Typed URL
Internet Explorer (Windows)	url8	05/01/13 11:30:55AM	http://www.rit.edu/news/nandedaily.php	Windows7	History\Typed URL
Internet Explorer (Windows)	url9	05/01/13 11:30:55AM	http://en.wikipedia.org/wiki/Main_Page	Windows7	History\Typed URL
Internet Explorer (Windows)	url10	05/01/13 11:30:55AM	http://go.microsoft.com/fwlink/?LinkId=69157	Windows7	History\Typed URL

Figure 14 Internet Explorer History

In addition to web browsing history, the records processor was able to uncover information regarding Internet Explorer bookmarks. During the data generation process I setup bookmarks within Internet Explorer for Live Email, Gmail, Twitter, Facebook, RIT News, and Wikipedia. This is confirmed by the fact that the records processor was able to find these exact bookmarks, though it is interesting that there appears to be many duplicates:

Browser Type	Created	Title	Url Name	Profile Name	Internet Artifact Type
Internet Explorer (Windows)	04/21/13 03:29:59PM	Live Email Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=1...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:59PM	Live Email Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=1...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:59PM	Live Email Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=1...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:59PM	Live Email Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=1...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:23PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:23PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:23PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:23PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:23PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:23PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&...	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:11PM	Twitter	https://twitter.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:11PM	Twitter	https://twitter.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:11PM	Twitter	https://twitter.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:11PM	Twitter	https://twitter.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:11PM	Twitter	https://twitter.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:29:11PM	Twitter	https://twitter.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:47PM	Welcome to Facebook - Log In, Sign ...	https://www.facebook.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:47PM	Welcome to Facebook - Log In, Sign ...	https://www.facebook.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:47PM	Welcome to Facebook - Log In, Sign ...	https://www.facebook.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:47PM	Welcome to Facebook - Log In, Sign ...	https://www.facebook.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:47PM	Welcome to Facebook - Log In, Sign ...	https://www.facebook.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:47PM	Welcome to Facebook - Log In, Sign ...	https://www.facebook.com/	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:19PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:19PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:19PM	RIT News - News & Events Daily		Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:19PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:19PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:28:19PM	RIT News - News & Events Daily		Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:27:31PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:27:31PM	Wikipedia, the free encyclopedia		Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:27:31PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows7	Bookmarks
Internet Explorer (Windows)	04/21/13 03:27:31PM	Wikipedia, the free encyclopedia		Windows7	Bookmarks

Figure 15 Internet Explorer Bookmarks

When I viewed what EnCase uncovered for Internet Explorer's Temporary Internet Files and Internet Cache I was surprised to find very few items related to web browsing. Instead I found numerous items pertaining to

what I believe to be Windows update downloads from http://downloads.microsoft.com. I am unsure why this information appears in this location as it would certainly hinder a true forensic investigation:

Browser Type	Url Name	Internet Artifact Type
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/A/D/6/AD6CFBFC-3A59-4C8C-8D89-8212B720BAE9/SetupPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/A/D/6/AD6CFBFC-3A59-4C8C-8D89-8212B720BAE9/SetupPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/7/0/A/70AABEC5-CCC0-40C8-BC09-CAE60F8E94E0/NrPolicy.cab	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/D/B/D/DBD62263-2627-49CB-B675-AA1601EBE0BD/Windows6.1-KB2454826-v2-x64.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/3/E/7/3E7F799A-DAB7-4CEF-A489-82B07337CBFF/NeutralMSU/amd64fre/IE9-win7.msu	Cache\Code
Internet Explorer (Windows)	http://download.microsoft.com/download/A/D/6/AD6CFBFC-3A59-4C8C-8D89-8212B720BAE9/SetupPolicy.cab	Cache\Code

Figure 16 Internet Explorer Cache

In addition to the information found regarding Windows updates, I was also able to uncover many of the images that were viewed or appeared on web pages that were viewed by the Windows 7 user:

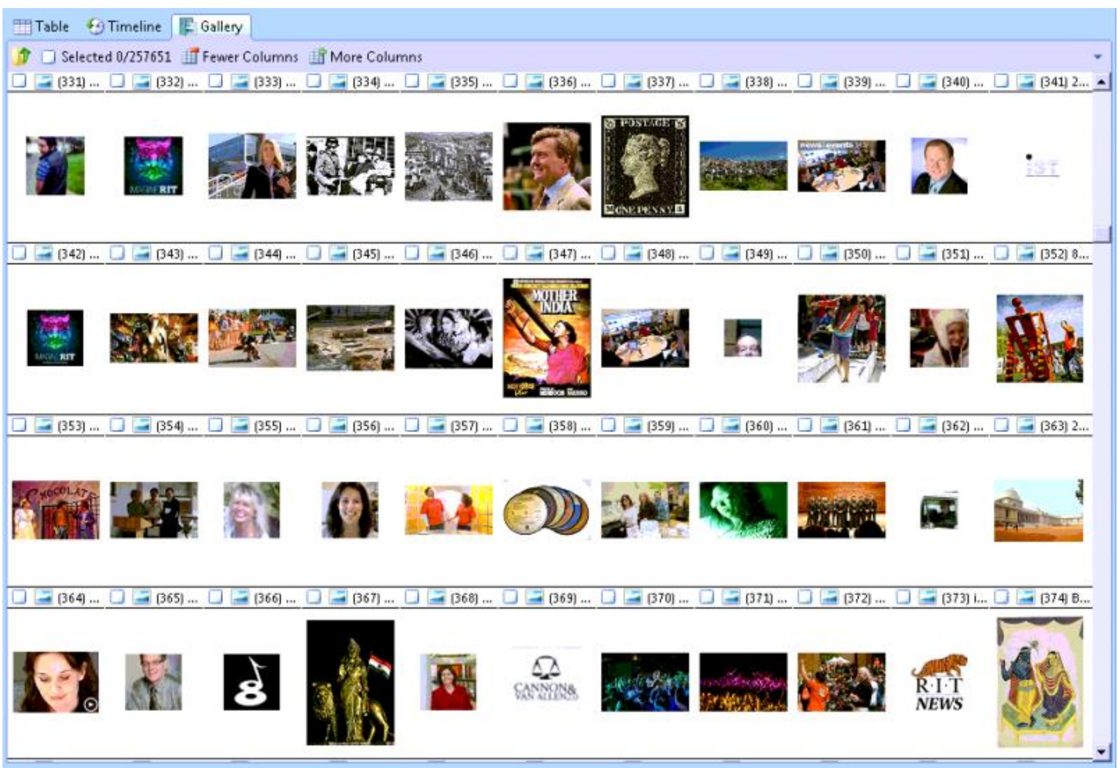


Figure 17 Internet Explorer Cached Images

Firefox

Uncovering information pertaining to the history, favorites, and cache of Firefox was just as simple as it was with Internet Explorer. However, instead of looking to a registry key, EnCase examined Firefox's sqlite databases located within user profiles. In this case, that location is C:\Users\Windows 7\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite. From these databases we are able to recover a complete browsing history for the Firefox browser. Unfortunately, EnCase was unable to display the time at which specific website were visited, but we can see that Facebook, Twitter, RIT News, Wikipedia, and other websites were visited during the data generation process using Firefox:

Browser Type	Title	Url Name	Internet Artifact Type
Mozilla 3 (Windows/Mac)	Untying the secret of Celtic knots - RIT News	http://www.rit.edu/news/story.php?id=49994&source=enew...	History
Mozilla 3 (Windows/Mac)	Facebook	https://www.facebook.com/	History
Mozilla 3 (Windows/Mac)	George Harrison - Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/George_Harrison	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	History
Mozilla 3 (Windows/Mac)	Google Accounts	https://accounts.google.com/ServiceLogin?service=chromiu...	History
Mozilla 3 (Windows/Mac)	Getting Started	http://tools.google.com/chrome/intl/en/welcome.html	History
Mozilla 3 (Windows/Mac)	Getting Started	https://www.google.com/intl/en/chrome/browser/welcome....	History
Mozilla 3 (Windows/Mac)		https://www.google.com/intl/en-US/chrome/blank.html?sou...	History
Mozilla 3 (Windows/Mac)		http://www.mozilla.com/en-US/firefox/20.0.1/firstrun/	History
Mozilla 3 (Windows/Mac)	Welcome to Firefox	http://www.mozilla.org/en-US/firefox/20.0.1/firstrun/	History
Mozilla 3 (Windows/Mac)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	History
Mozilla 3 (Windows/Mac)	Reginald Heber - Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Reginald_Heber	History
Mozilla 3 (Windows/Mac)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	History
Mozilla 3 (Windows/Mac)	RIT screening of award-winning film 'United in Anger' debuts April...	http://www.rit.edu/news/story.php?id=49951&source=enew...	History
Mozilla 3 (Windows/Mac)	Pollution Prevention Institute recognizes Brooklyn Navy Yard for en...	http://www.rit.edu/news/story.php?id=49953&source=enew...	History
Mozilla 3 (Windows/Mac)	Facebook	https://www.facebook.com/	History
Mozilla 3 (Windows/Mac)	Facebook	http://www.facebook.com/?sk=welcome	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	History
Mozilla 3 (Windows/Mac)	Facebook	https://www.facebook.com/	History
Mozilla 3 (Windows/Mac)		http://www.facebook.com/index.php?stype=lo&jlou=AffFPiy...	History
Mozilla 3 (Windows/Mac)	Welcome to Facebook - Log In, Sign Up or Learn More	https://www.facebook.com/index.php?stype=lo&jlou=AffFPi...	History
Mozilla 3 (Windows/Mac)	Facebook	http://www.facebook.com/?sk=welcome	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	History
Mozilla 3 (Windows/Mac)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	History
Mozilla 3 (Windows/Mac)	Alcohol laws of New Jersey - Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Alcohol_laws_of_New_Jersey	History
Mozilla 3 (Windows/Mac)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	History
Mozilla 3 (Windows/Mac)	Maya Angelou Program at RIT Canceled - RIT News	http://www.rit.edu/news/story.php?id=49963&source=enew...	History
Mozilla 3 (Windows/Mac)	RIT wins National Collegiate Cyber Defense Competition for the fir...	http://www.rit.edu/news/story.php?id=49964&source=enew...	History
Mozilla 3 (Windows/Mac)	It's not too late to 'Live United' by donating to RIT's 2013 campaig...	http://www.rit.edu/news/story.php?id=49962&source=enew...	History

Figure 18 Firefox History

As previously mentioned the places.sqlite database files contain information regarding web browsing history; that file also contains information pertaining to a user's Firefox bookmarks. From the EnCase records processor we can see that Facebook, RIT News, Twitter, and Wikipedia are among the Firefox bookmarks on the Windows 7 virtual machine:

Browser Type	Created	Title	Url Name	Internet Artifact Type
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Facebook	https://www.facebook.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Facebook	https://www.facebook.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Facebook	https://www.facebook.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Facebook	https://www.facebook.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Twitter	https://twitter.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Twitter	https://twitter.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Twitter	https://twitter.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Twitter	https://twitter.com/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		http://www.mozilla.com/en-US/about/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		https://accounts.google.com/ServiceLogin?service=mail&pas...	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&c...	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM			Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM			Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM			Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM			Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM			Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM			Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		http://www.mozilla.com/en-US/firefox/help/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		http://www.mozilla.com/en-US/firefox/customize/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		http://www.mozilla.com/en-US/firefox/community/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		http://www.mozilla.com/en-US/about/	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 03:34:07PM		place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKM...	Bookmarks

Figure 19 Firefox Favorites

Viewing Firefox's web cache or temporary Internet files can be found within C:\Users\Windows 7\AppData\Local\Mozilla\Firefox\Profiles\<random text>.default\Cache. EnCase then examined the files contained within the directory and uncovered cached pages for RIT, Twitter, Google, and several other web sites:

Browser Type	Created	Url Name	Internet Artifact Type
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/featured/poster_winner_2013.jpg	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/featured/poster_winner_2013.jpg	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/featured/exhibit-elspeth.jpg	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/featured/edurance_feature.jpg	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/countdown_bubble.png	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/suckerfish-hover.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/subpages/index2.jpg	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/	Cache\HTML
Mozilla (Windows/Mac)	05/04/13 03:39:19PM	http://www.rit.edu/imagine/images/featured/itinerary2012.jpg	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:38:52PM	https://platform.twitter.com/widgets/hub.html	Cache\HTML
Mozilla (Windows/Mac)	05/04/13 03:38:52PM	http://platform.twitter.com/widgets/hub.html	Cache\HTML
Mozilla (Windows/Mac)	05/04/13 03:38:52PM	http://platform.twitter.com/widgets/hub.html	Cache\HTML
Mozilla (Windows/Mac)	05/04/13 03:38:52PM	https://platform.twitter.com/widgets/hub.html	Cache\HTML
Mozilla (Windows/Mac)	05/04/13 03:38:51PM	http://platform.twitter.com/js/tfw/hub/client.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:51PM	http://platform.twitter.com/js/tfw/hub/client.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://api-public.addthis.com/url/shares.json?url=http%3A%2F%2Fwww.rit.edu%2Fnews%2Fstory.php%3Fid%3D49994...	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://platform.twitter.com/widgets.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://apis.google.com/js/plusone.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://api-public.addthis.com/url/shares.json?url=http%3A%2F%2Fwww.rit.edu%2Fnews%2Fstory.php%3Fid%3D49994...	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://p.twitter.com/t.gif?_=1367696283870&count=horizontal&counturl=http%3A%2F%2Fwww.rit.edu%2Fnews%2Fst...	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://cdn.api.twitter.com/1/urls/count.json?url=http%3A%2F%2Fwww.rit.edu%2Fnews%2Fstory.php%3Fid%3D49994...	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://platform.twitter.com/widgets.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://apis.google.com/js/plusone.js	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://p.twitter.com/t.gif?_=1367696283870&count=horizontal&counturl=http%3A%2F%2Fwww.rit.edu%2Fnews%2Fst...	Cache\Image
Mozilla (Windows/Mac)	05/04/13 03:38:49PM	http://cdn.api.twitter.com/1/urls/count.json?url=http%3A%2F%2Fwww.rit.edu%2Fnews%2Fstory.php%3Fid%3D49994...	Cache\Code
Mozilla (Windows/Mac)	05/04/13 03:38:48PM	http://s7.addthis.com/js/250/addthis_widget.js	Cache\Code

Figure 20 Firefox Cache

When I took a look at the gallery option for Firefox's web cache, I found images from the many websites visited during the data generation process:

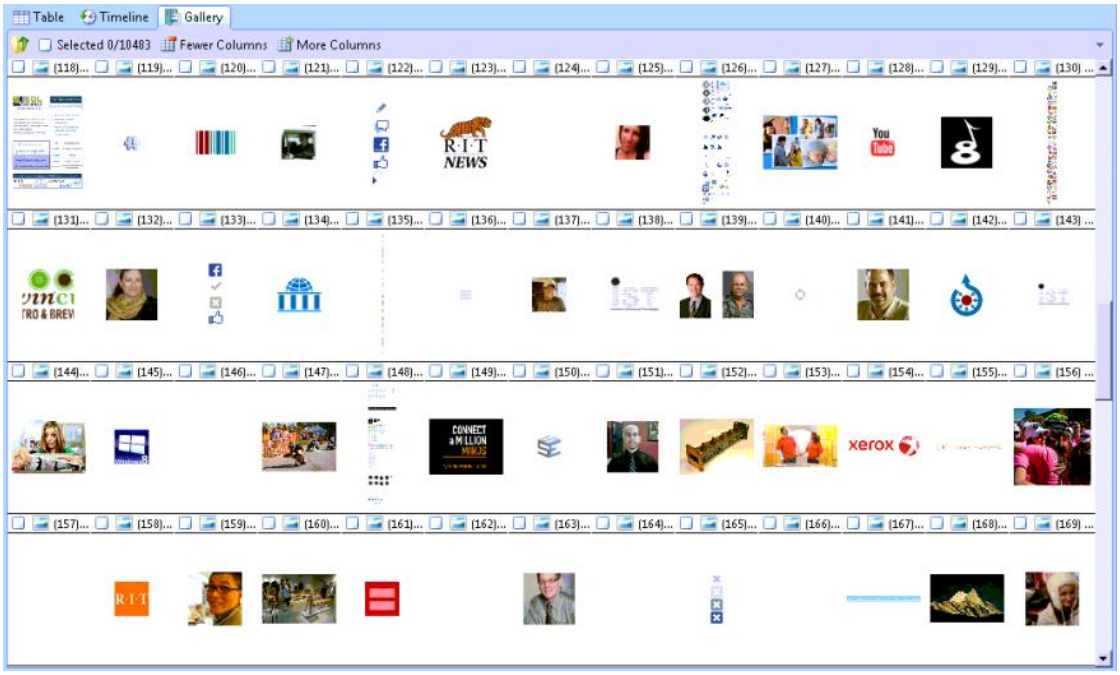


Figure 21 Firefox Cached Images

One of the more interesting artifacts that I was able to find using the EnCase records processor was information regarding Firefox login data. It appears that Firefox stored information regarding Facebook login credentials. This is especially interesting because I instructed Firefox to remember usernames and passwords for both Facebook and Twitter; yet EnCase only found the stored Facebook credentials. It should be noted that these credentials are not stored in plaintext. The values of the username and password are encrypted:

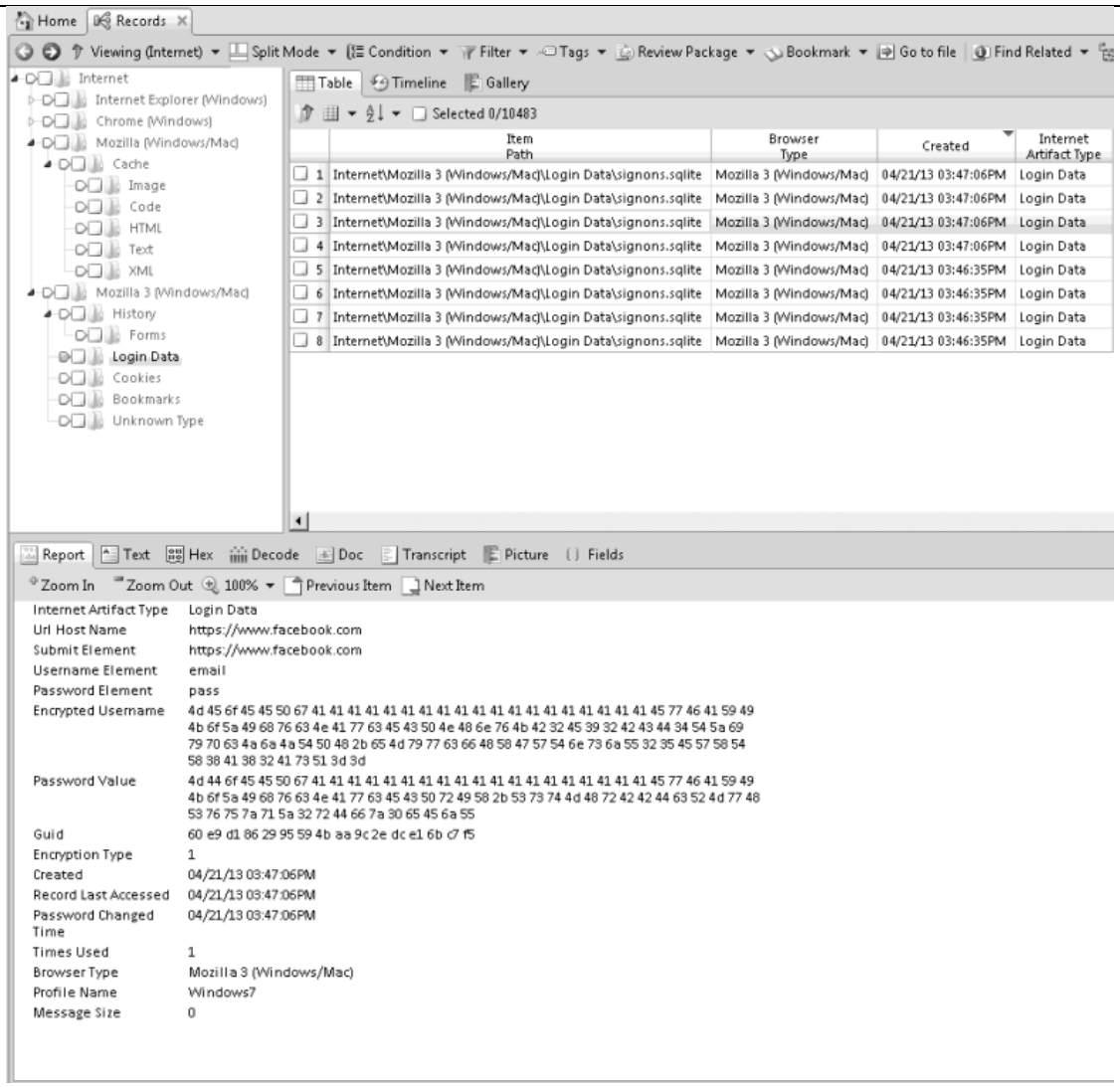


Figure 22 Firefox Stored Login Data

Chrome

Like Firefox, the Chrome web browser stores information within the user's profile. In the case of the Wndows 7 virtual machine, that location is C:\Users\AppData\Windows 7\Local\Google\User Data. From this directory, we are able to find history, favorites, and cache of Chrome. Using the EnCase records processor I was able to recover a complete browsing history for Chrome with accessed date/time. We are able to see that during the data generation process Chrome was used to visit Twitter, RIT News, Facebook, Wikipedia, and several other websites:

Browser Type	Title	Accessed	Url Name	Internet Artifact Type
Chrome (Windows)	Twitter	05/04/13 03:42:49PM	https://twitter.com/	History
Chrome (Windows)	Twitter	05/04/13 03:42:49PM	https://twitter.com/	History
Chrome (Windows)	Untying the secret of Celtic knots - RIT News	05/04/13 03:40:12PM	http://www.rit.edu/news/story.php?id=49994&source=enew...	History
Chrome (Windows)	RIT - Imagine RIT: Innovation and Creativity Festival	05/04/13 03:40:12PM	http://www.rit.edu/imagine/	History
Chrome (Windows)	RIT - Imagine RIT: Innovation and Creativity Festival	05/04/13 03:40:12PM	http://www.rit.edu/imagine/	History
Chrome (Windows)	Untying the secret of Celtic knots - RIT News	05/04/13 03:40:12PM	http://www.rit.edu/news/story.php?id=49994&source=enew...	History
Chrome (Windows)	Facebook	05/04/13 03:39:44PM	https://www.facebook.com/	History
Chrome (Windows)	Facebook	05/04/13 03:39:44PM	https://www.facebook.com/	History
Chrome (Windows)	George Harrison - Wikipedia, the free encyclopedia	05/04/13 03:39:33PM	http://en.wikipedia.org/wiki/George_Harrison	History
Chrome (Windows)	George Harrison - Wikipedia, the free encyclopedia	05/04/13 03:39:33PM	http://en.wikipedia.org/wiki/George_Harrison	History
Chrome (Windows)	Wikipedia, the free encyclopedia	05/04/13 03:39:27PM	http://en.wikipedia.org/wiki/Main_Page	History
Chrome (Windows)	Wikipedia, the free encyclopedia	05/04/13 03:39:27PM	http://en.wikipedia.org/wiki/Main_Page	History
Chrome (Windows)	Facebook	05/04/13 03:39:25PM	https://www.facebook.com/	History
Chrome (Windows)	Facebook	05/04/13 03:39:25PM	https://www.facebook.com/	History
Chrome (Windows)	Twitter	05/04/13 03:39:23PM	https://twitter.com/	History
Chrome (Windows)	Twitter	05/04/13 03:39:23PM	https://twitter.com/	History
Chrome (Windows)	RIT News - News & Events Daily	05/04/13 03:39:20PM	http://www.rit.edu/news/nandedaily.php	History
Chrome (Windows)	RIT News - News & Events Daily	05/04/13 03:39:20PM	http://www.rit.edu/news/nandedaily.php	History
Chrome (Windows)	Twitter	05/03/13 04:45:52PM	https://twitter.com/	History
Chrome (Windows)	Twitter	05/03/13 04:45:52PM	https://twitter.com/	History
Chrome (Windows)	Keith Motley, University of Massachusetts chancellor, keynotes R...	05/03/13 04:42:24PM	http://www.rit.edu/news/story.php?id=49957&source=enew...	History
Chrome (Windows)	Keith Motley, University of Massachusetts chancellor, keynotes R...	05/03/13 04:42:24PM	http://www.rit.edu/news/story.php?id=49957&source=enew...	History
Chrome (Windows)	Eight Beat Measure celebrates 25 years - RIT News	05/03/13 04:42:21PM	http://www.rit.edu/news/story.php?id=49993&source=enew...	History
Chrome (Windows)	Eight Beat Measure celebrates 25 years - RIT News	05/03/13 04:42:21PM	http://www.rit.edu/news/story.php?id=49993&source=enew...	History
Chrome (Windows)	RIT's 2013 Innovation Hall of Fame induction is Friday - RIT News	05/03/13 04:42:17PM	http://www.rit.edu/news/story.php?id=49992&source=enew...	History
Chrome (Windows)	RIT's 2013 Innovation Hall of Fame induction is Friday - RIT News	05/03/13 04:42:17PM	http://www.rit.edu/news/story.php?id=49992&source=enew...	History
Chrome (Windows)	Facebook	05/03/13 04:41:37PM	https://www.facebook.com/	History

Figure 23 Chrome History

EnCase easily uncovered the Windows 7 user's Top Sites, which include that user's favorites/bookmarks. In the case of the Window s7 virtual machine we see that Chrome frequently visited Wikipedia, the RIT Mirrors, RIT News, Twitter, and Facebook:

Browser Type	Title	Url Name	Internet Artifact Type
Chrome (Windows)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Top Sites
Chrome (Windows)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Top Sites
Chrome (Windows)	Index of /	http://mirrors.rit.edu/	Top Sites
Chrome (Windows)	Index of /	http://mirrors.rit.edu/	Top Sites
Chrome (Windows)	Welcome to Google Chrome	http://www.google.com/chrome/intl/en/welcome.html	Top Sites
Chrome (Windows)	Welcome to Google Chrome	http://www.google.com/chrome/intl/en/welcome.html	Top Sites
Chrome (Windows)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Top Sites
Chrome (Windows)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Top Sites
Chrome (Windows)	Chrome Web Store	https://chrome.google.com/webstore?hl=en	Top Sites
Chrome (Windows)	Chrome Web Store	https://chrome.google.com/webstore?hl=en	Top Sites
Chrome (Windows)	Twitter	https://twitter.com/	Top Sites
Chrome (Windows)	Twitter	https://twitter.com/	Top Sites
Chrome (Windows)	(1) Facebook	https://www.facebook.com/	Top Sites
Chrome (Windows)	(1) Facebook	https://www.facebook.com/	Top Sites

Figure 24 Chrome Top Sites

From the Chrome User Data directory along with EnCase, it was simple to uncover a listing of web pages that were visited by the user through the use of Chrome's web cache. From this we can see that during the data generation process I visited Wikipedia, Facebook, Twitter, RIT, and many other websites:

Browser Type	Created	Url Name	Internet Artifact Type
Chrome (Windows)	05/03/13 04:42:25PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/ys/r/fnBZhAgqpcM.png	Cache\Image
Chrome (Windows)	05/04/13 03:40:20PM	http://upload.wikimedia.org/wikipedia/commons/thumb/d/d6/Wikiquote-logo-en.svg/40px-Wikiquote-logo-en...	Cache\Image
Chrome (Windows)	05/04/13 03:40:29PM	https://fbcdn-creative-a.akamaihd.net/hads-ak-ash3/s110x80/735327_6007144937656_507415288_n.png	Cache\Image
Chrome (Windows)	05/03/13 04:42:19PM	http://www.rit.edu/news/images/blog.gif	Cache\Image
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/sponsors2010/rghs.gif	Cache\Image
Chrome (Windows)	05/04/13 03:41:03PM	http://profile.ak.fbcdn.net/hprofile-ak-prn1/48824_732486294_342702120_q.jpg	Cache\Image
Chrome (Windows)	05/04/13 03:40:07PM	http://meta.wikimedia.org/wiki/Special:RecordImpression?result=hide&reason=empty&country=US&uselang=...	Cache\Image
Chrome (Windows)	05/04/13 03:40:30PM	https://fbcdn-sphotos-e-a.akamaihd.net/hphotos-ak-ash4/s480x480/485400_10151352916191930_2119440542_n...	Cache\Image
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/sponsors2011/hp.gif	Cache\Image
Chrome (Windows)	05/04/13 03:41:00PM	http://farm9.staticflickr.com/8268/8706880044_d355128ec7_s.jpg	Cache\Image
Chrome (Windows)	05/04/13 03:41:03PM	http://profile.ak.fbcdn.net/hprofile-ak-frc1/275407_100005370100122_1057571410_q.jpg	Cache\Image
Chrome (Windows)	05/03/13 04:42:23PM	https://twimg0-a.akamaihd.net/sticky/default_profile_images/default_profile_6_mini.png	Cache\Image
Chrome (Windows)	05/04/13 03:40:15PM	http://upload.wikimedia.org/wikipedia/en/b/bc/Wiki.png	Cache\Image
Chrome (Windows)	05/03/13 04:43:12PM	http://www.rit.edu/news/lib/filelib/201305/smithtaylor.jpg	Cache\Image
Chrome (Windows)	05/03/13 04:42:24PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/y9/r/jKEcVPZFk-2.gif	Cache\Image
Chrome (Windows)	05/03/13 04:42:26PM	https://www.facebook.com/images/spacer.gif	Cache\Image
Chrome (Windows)	05/03/13 04:42:18PM	http://www.rit.edu/news/images/daily/header-20130503.jpg?1882678350	Cache\Image
Chrome (Windows)	05/03/13 04:42:26PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/yA/r/4WSewcWboV8.png	Cache\Image
Chrome (Windows)	05/02/13 03:14:24PM	http://l.yimg.com/a/i/us/we/52/28.gif	Cache\Image
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/nav-right.gif	Cache\Image
Chrome (Windows)	05/03/13 04:43:12PM	http://www.rit.edu/news/lib/filelib/201305/pancarischott.jpg	Cache\Image
Chrome (Windows)	05/03/13 04:42:28PM	https://fbcdn-profile-a.akamaihd.net/hprofile-ak-frc1/s32x32/275407_100005370100122_1057571410_q.jpg	Cache\Image
Chrome (Windows)	05/04/13 03:40:28PM	https://fbcdn-sphotos-c-a.akamaihd.net/hphotos-ak-ash3/s480x480/945622_639276886086846_1111833439_n.jpg	Cache\Image
Chrome (Windows)	05/03/13 04:42:18PM	http://www.rit.edu/_files/bodyBG.gif	Cache\Image
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/2012-header.gif	Cache\Image
Chrome (Windows)	05/03/13 04:42:24PM	http://www.rit.edu/_files/footer.gif	Cache\Image

Figure 25 Chrome Cache

When I took a look at the gallery option for Chrome's web cache, I found images from the many websites visited during the data generation process:

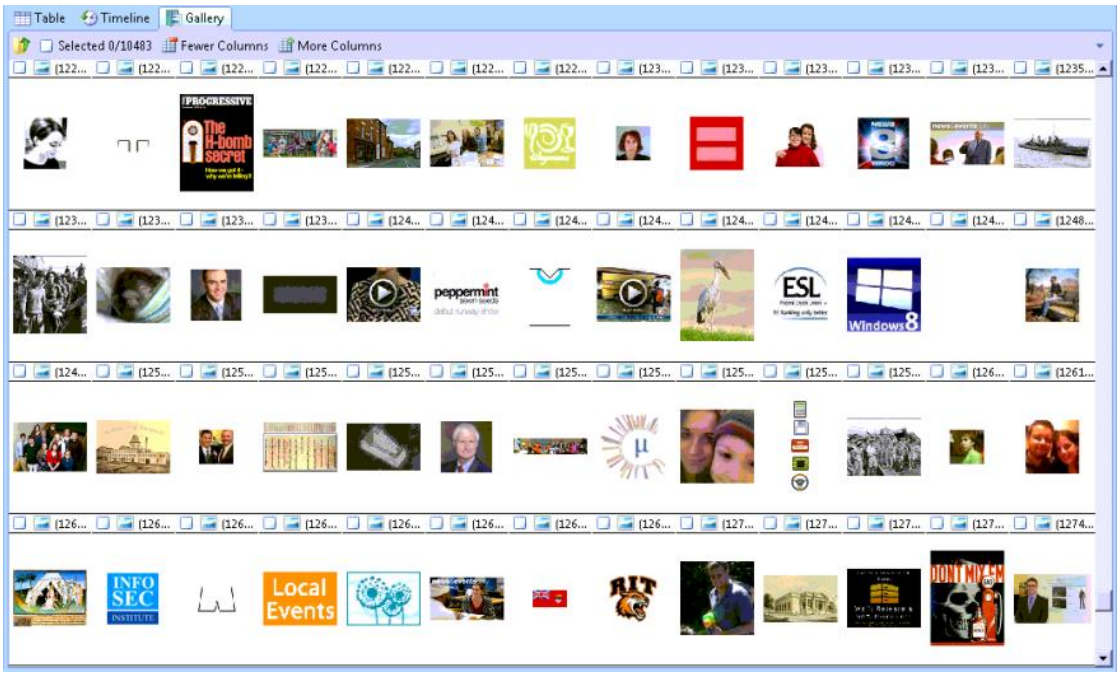


Figure 26 Chrome Cached Images

As was the case with Firefox, Chrome also contained interesting artifacts regarding Chrome login data. It appears that Chrome stored information regarding Facebook and Twitter login credentials. This makes more sense than what I saw with Firefox as I instructed Chrome to remember usernames and passwords for both Facebook and Twitter. As was the case with Firefox and Facebook, the username and password credentials are not stored in

plaintext. The values of the username and password are encrypted. What is interesting is the fact that with Twitter the user is stored in plaintext but the password value is encrypted:

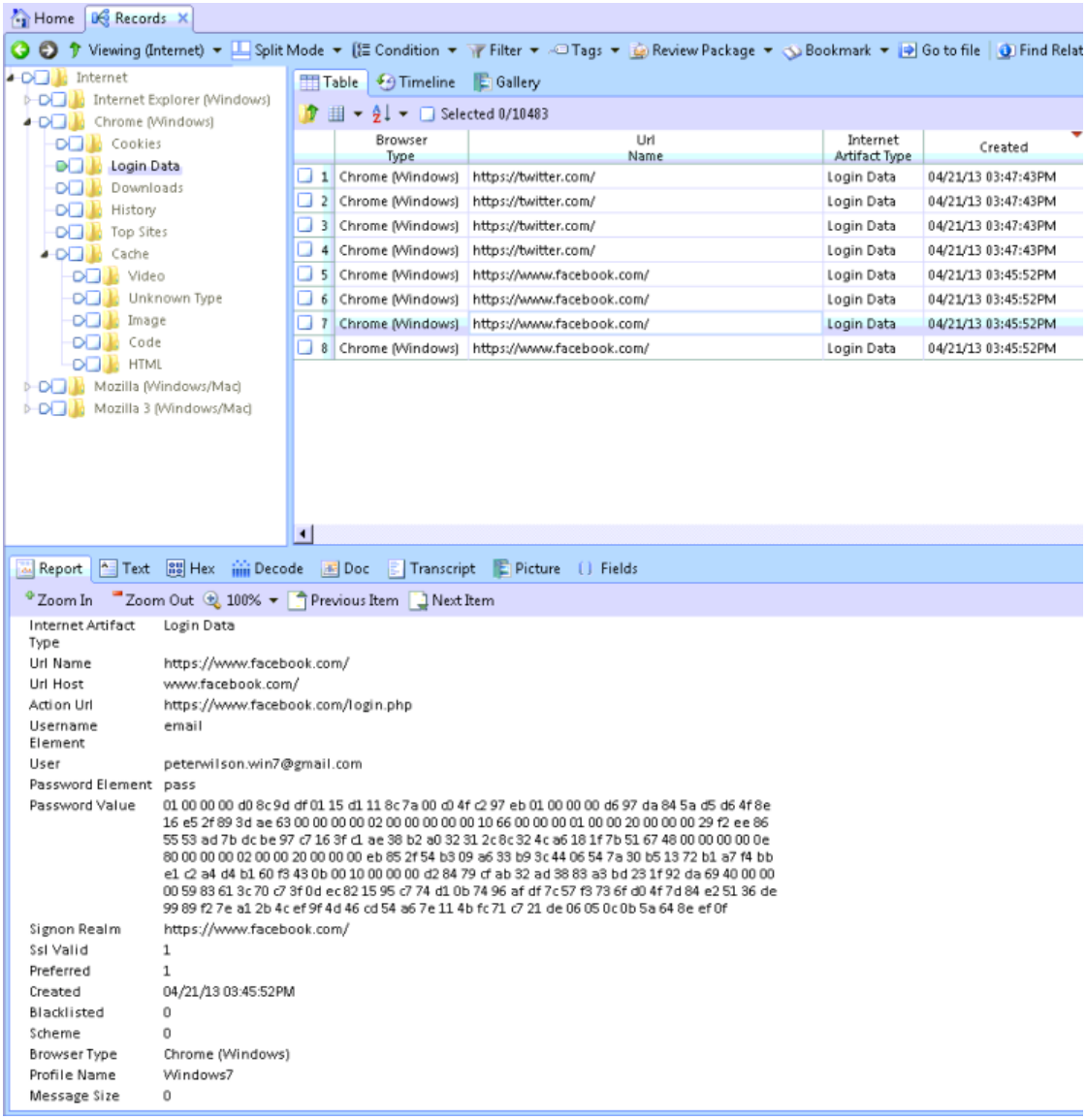


Figure 27 Chrome Login Data

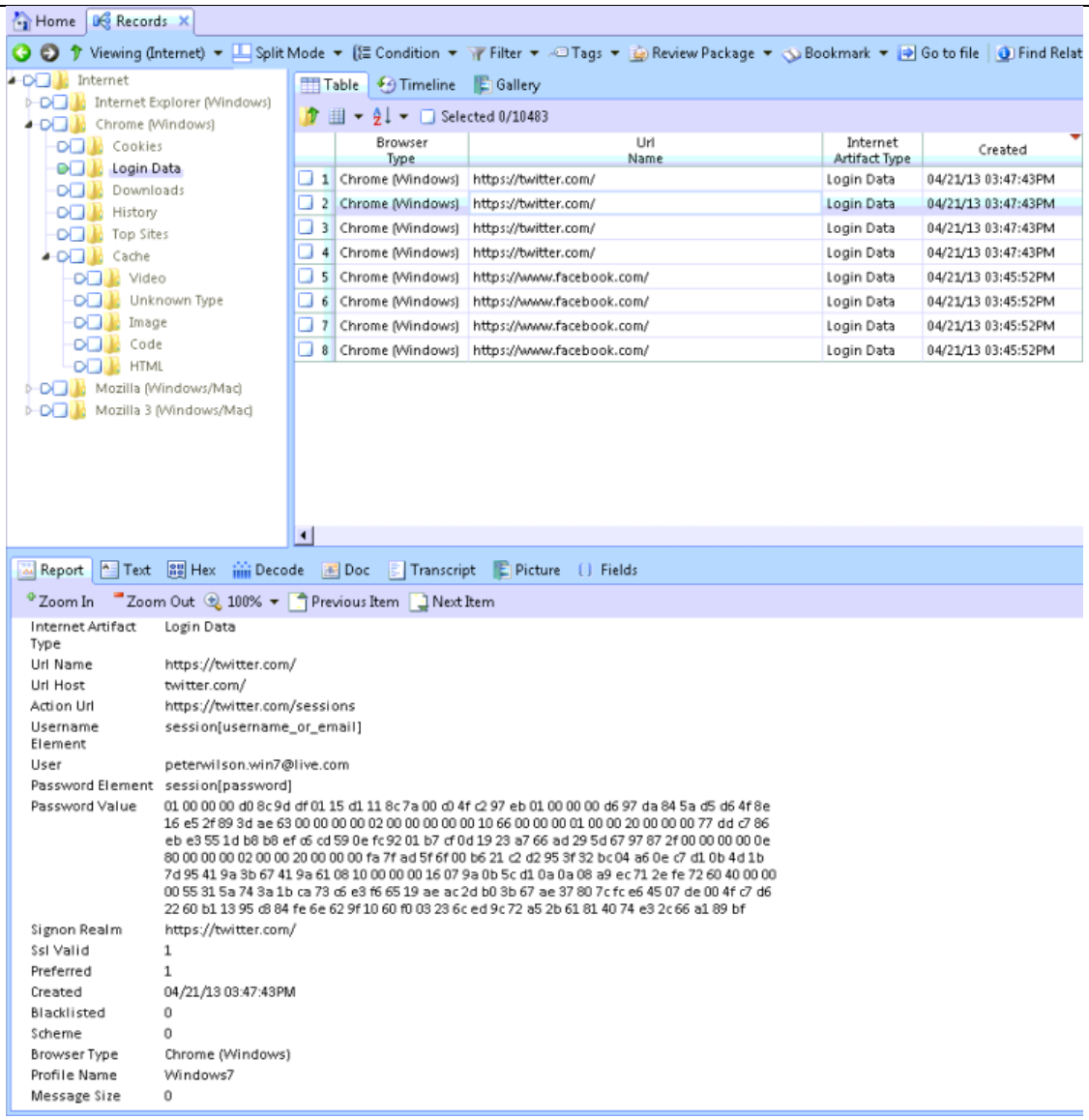


Figure 28 Chrome Login Data

Social Media Items

Finding evidence of social media with FTK wasn't especially difficult. With FTK, I used the Live Search feature along with the keywords "facebook" and "twitter". This enabled be to find artifacts pertaining to those two social media websites. The live search found a total of 8283 hits for the, case insensitive, ANSI, keyword "facebook" within 520 files and 7955 hits for the, case insensitive, ANSI, keyword "twitter" within 336 files:

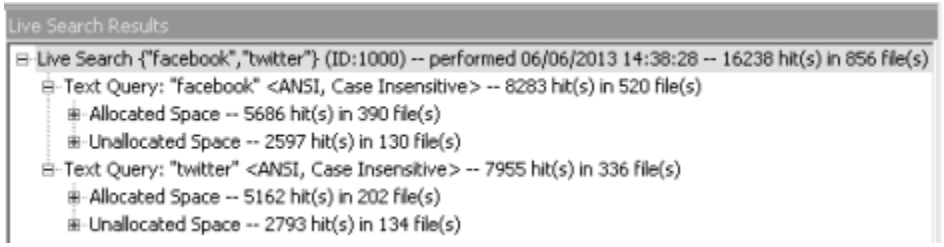


Figure 29 Social Media Items

The majority of the files that I found that contained mention of either Facebook or Twitter were primarily the result of browsing to websites that contained options to share the contents via Facebook or Twitter. There were numerous files with htm, js, css, tmp, and other file extensions but I was unable to uncover any of the specific social media actions that I took during the data generation process.

While I found quite a bit of evidence that the social media sites of Facebook and Twitter were used, I was unable to uncover any actual Facebook posts, shares, comments, or likes or Twitter tweets, retweets, replies, or favorites. I believe this is the case because the only way through which I accessed the social media sites was through web browsers. While I made updates to social media throughout the course of the data generation process, I suspect very little was actually stored on the hard drive of the Windows 7 virtual machine.

Internet Evidence Finder

Because FTK and EnCase were unable to easily locate evidence pertaining to Internet activity including social media usage, I opted to use Magnet Forensics' Internet Evidence Finder (IEF). This tool was extremely useful in uncover data related to social media activities, finding numerous items for many different, important, categories:

Internet Evidence Finder v6.1
Copyright 2009-2013 Magnet Forensics® Inc.
Build 6.1.1.0033
Case Information Generated At: 08/19/2013 16:14:16
Operating System: Microsoft Windows NT 6.1.7601 Service Pack 1

Selected source:

Windows 7.vmdk - Partition 1 (Microsoft NTFS, 40 GB)

Searches selected:
---
pagefile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:

Windows 7.vmdk - Unpartitioned Space

Searches selected:

Unpartitioned Space

Search items selected:

Browser Activity

Chrome

Facebook Chat

Facebook Email

Facebook Email 'Snippets'

Facebook Pictures

Facebook Status Updates / Wall Posts / Comments

Facebook Web Page Fragments

Firefox

Flash Video Fragments

Gmail

Google Maps

Google Plus

GoogleDocs

GoogleDrive

Hotmail

Internet Explorer 10 History

Internet Explorer v5-9

Internet Explorer v7-v10 InPrivate/Recovery URLs

Pictures

RebuildWeb

SkyDrive

Twitter

Videos

Webpage Recovery

Output folder: E:\Windows 7 IEF\IEF - Windows7\

Start time: Aug 19, 2013 16:14:16

End time: Aug 19, 2013 22:24:58

Duration: 06:10:41

Final results of search:

Internet Explorer 10 Carved History: 2169 items

Pictures: 35110 items

Browser Activity: 4938 items

Facebook URLs: 1189 items

Social Media URLs: 694 items

Parsed Search Queries: 305 items

Cloud Services URLs: 5 items

Internet Explorer 10 Carved Content Records: 11332 items

IE InPrivate/Recovery URLs: 370 items

Facebook Pages: 5 items

Facebook Status Updates/Wall Posts/Comments: 49 items

Internet Explorer Cache Records Carved: 7 items

Internet Explorer Typed URLs: 10 items

Videos: 164 items

Internet Explorer Redirect Records: 11 items

Internet Explorer Cookie Records: 2 items

Internet Explorer Cookies: 176 items

Internet Explorer 10 History: 595 items

Internet Explorer 10 Content: 2596 items

Rebuilt Webpages: 187 items

Chrome Bookmarks: 6 items

Chrome Cookies: 76 items

Chrome FavIcons: 65 items

Chrome Web History: 195 items

Chrome History Index: 80 items

Chrome/360 Safe Browser Carved Web History: 261 items

Chrome Logins: 2 items

Chrome Top Sites: 7 items

Chrome Autofill: 2 items

Internet Explorer Cache Records: 6 items

Firefox Cookies: 73 items

Firefox FormHistory: 2 items

Firefox Web History: 102 items

Firefox Bookmarks: 17 items

Firefox FavIcons: 12 items

Firefox Downloads: 1 items

Firefox SessionStore Artifacts: 145 items

Chrome Cache Records: 425 items

Internet Explorer 10 Cookies: 54 items

Dating Sites URLs: 5 items

Firefox Cache Records: 1500 items

Facebook Pictures: 155 items

Google Maps: 4 items

Twitter: 24 items

Firefox Carved FormHistory: 1 items

Figure 30 Windows 7 IEF Case Summary

Facebook Activity

Using IEF, I was able to uncover a total of 11 posts or comments that were made as part of the data generation process. Some of the posts or comments were made by the WindowsSeven Forensics Facebook user, while others were made by the WindowsEight Forensics user. I believe this is the case because these two fictional users were friends with each other on Facebook so they would have seen each other's posts and/or comments. I find it especially interesting that when an actual post is made the Sender Name is known, but the Date/Time when it was posted is not, whereas when a comment is made, the Sender Name is unknown, but the Date/Time is. In the figure below, the 11 posts/comments can be seen.

	Sender ID	Sender Name	Status Update / Wall Post / Comment	Posted Date/Time - (UTC) (MM/dd/yyyy)	Source	Located At
★	12	100005370100122	WindowsSeven Forensics	04/23/2013 Daily Post From Firefox	Windows 7.vmdk - Partition 1 ...	File offset 624101321
☆	13	100005359690264	WindowsEight Forensics	4/21/2013 Daily Post From Chrome	Windows 7.vmdk - Partition 1 ...	File offset 624106682
☆	28	100005370100122	WindowsSeven Forensics	05/03/2013 Daily Post From Internet Explorer	Windows 7.vmdk - Partition 1 ...	Physical Sector 4235147
☆	32	100005359690264	WindowsEight Forensics	05/02/2013 Daily post From Firefox	Windows 7.vmdk - Partition 1 ...	Physical Sector 4235192
☆	34	100005370100122	n/a	Comment From Internet Explorer	05/03/2013 08:47:33 PM	Windows 7.vmdk - Partition 1 ...	Physical Sector 32981194
☆	35	100005359690264	n/a	Comment from Firefox	05/02/2013 03:33:18 PM	Windows 7.vmdk - Partition 1 ...	Physical Sector 32981199
☆	36	100005359690264	n/a	Comment from People App	05/03/2013 11:09:50 PM	Windows 7.vmdk - Partition 1 ...	Physical Sector 32981204
☆	41	100005370100122	WindowsSeven Forensics	05/02/2013 Daily Post from Firefox	Windows 7.vmdk - Partition 1 ...	Physical Sector 33057200
☆	42	100005359690264	WindowsEight Forensics	05/01/2013 Daily Post From Chrome	Windows 7.vmdk - Partition 1 ...	Physical Sector 33057211
☆	43	100005370100122	n/a	Comment from Firefox	05/02/2013 03:17:13 PM	Windows 7.vmdk - Partition 1 ...	Physical Sector 33057239
☆	44	100005359690264	n/a	Comment from Internet Explorer App	05/01/2013 03:52:05 PM	Windows 7.vmdk - Partition 1 ...	Physical Sector 33057244

Figure 31 Windows 7 Facebook Activity

Twitter Activity

Using IEF, I was able to uncover a total of 17 tweets and retweets that were made or viewed as part of the data generation process. IEF was able to discover 16 total tweets made from @RITsports or @RIT_SportsZone that were made yet only a single tweet from @Win7Forensics. The tweets that are seen, are from the Twitter feed of @Win7Forensics that was accessed through twitter.com as part of the data generation process.

	Name	Screen Name	Created Date/Time - (UTC) (MM/dd/yyyy)	Tweet Text	Source	Located At
★	1	RIT Sports Info	@RITsports	05/02/2013 02:12:38 AM	BB | <a href="/search?q=%23RIT&src=hash" data-q...	Windows 7.vmdk - Partition 1 ...	File offset 120863226
☆	3	RIT Sports Info	@RITsports	05/04/2013 05:52:21 PM	<a href="/search?q=%23LLWTennisChampionship&...	Windows 7.vmdk - Partition 1 ...	Physical Sector 2923740
☆	5	RIT NEWS	@RITNEWS	05/04/2013 05:19:39 PM	Coverage of <a href="/Imagine_RIT" class="twitter-...	Windows 7.vmdk - Partition 1 ...	Physical Sector 2923765
☆	7	RIT Sports Info	@RITsports	05/04/2013 04:34:42 PM	BB | <a href="/search?q=%23RIT&src=hash" class=...	Windows 7.vmdk - Partition 1 ...	Physical Sector 2923794
☆	10	RIT Sports Info	@RITsports	05/04/2013 04:21:47 PM	<a href="/search?q=%23LLWTennisChampionship&...	Windows 7.vmdk - Partition 1 ...	Physical Sector 2923838
☆	11	RIT Sports Info	@RITsports	05/04/2013 04:16:25 PM	BB | <a href="/search?q=%23RIT&src=hash" class=...	Windows 7.vmdk - Partition 1 ...	Physical Sector 2923851
☆	13	Windows 7 Forensics	@Win7Forensics	05/04/2013 07:44:05 PM	05/04/2013 Daily Tweet from Firefox	Windows 7.vmdk - Partition 1 ...	Physical Sector 30302578
☆	14	RIT Sports Info	@RITsports	05/04/2013 07:42:14 PM	U of R scores in the bottom of the 5th to tie the gam...	Windows 7.vmdk - Partition 1 ...	Physical Sector 30400054
☆	15	RIT Sports Info	@RITsports	05/04/2013 07:17:30 PM	<a href="/search?q=%23RIT&src=hash" class="twitt...	Windows 7.vmdk - Partition 1 ...	Physical Sector 30401964
☆	16	RIT Sports Info	@RITsports	05/04/2013 07:11:51 PM	<a href="/search?q=%23RIT&src=hash" class="twitt...	Windows 7.vmdk - Partition 1 ...	Physical Sector 30401977
☆	17	RIT Sports Info	@RITsports	05/04/2013 06:57:06 PM	<a href="/search?q=%23LLWTennisChampionship&...	Windows 7.vmdk - Partition 1 ...	Physical Sector 30401989
☆	18	RIT Sports Info	@RITsports	05/04/2013 06:54:48 PM	<a href="/search?q=%23LLWTennisChampionship&...	Windows 7.vmdk - Partition 1 ...	Physical Sector 30402001
☆	19	RIT NEWS	@RITNEWS	04/23/2013 06:30:15 PM	<a href="/search?q=%23RIT&src=hash" data-query-...	Windows 7.vmdk - Partition 1 ...	Physical Sector 31080725
☆	21	RIT Sports Info	@RITsports	04/25/2013 10:41:21 PM	BB | <a href="/search?q=%23RIT&src=hash" data-q...	Windows 7.vmdk - Partition 1 ...	Physical Sector 50094657
☆	22	RIT SportsZone	@RIT_SportsZone	04/26/2013 03:39:04 PM	New episode features interviews with MLax freshma...	Windows 7.vmdk - Partition 1 ...	Physical Sector 50279709
☆	23	RIT Sports Info	@RITsports	04/21/2013 07:17:54 PM	<a href="/search?q=%23RIT&src=hash" data-query-...	Windows 7.vmdk - Partition 1 ...	Physical Sector 50280062
☆	24	RIT Sports Info	@RITsports	04/21/2013 07:17:54 PM	<a href="/search?q=%23RIT&src=hash" data-query-...	Windows 7.vmdk - Partition 1 ...	Physical Sector 16155230

Figure 32 Windows 7 Twitter Activity

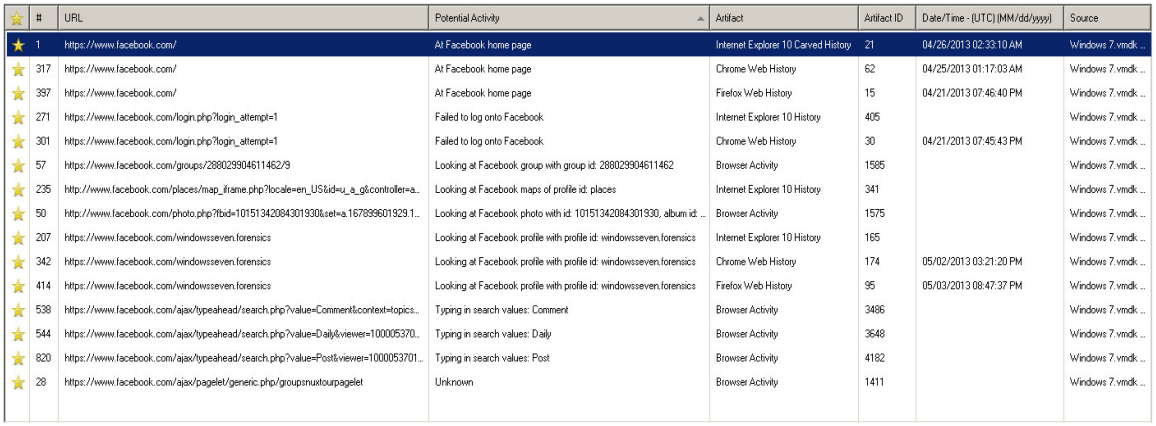
Facebook URLs

While using IEF, I was able to uncover 1189 specific Facebook URLs from Carved History or ecorded Browser Activity including the following potential activities:

- At Facebook home page
- Failed to log onto Facebook
- Looking at Facebook group…
- Looking at Facebook maps…
- Looking at Facebook photo…

- Looking at Facebook profile…
- Typing in search values:
- Unknown

These 8 different types of potential activities are categories that IEF uses to classify the data that it has carved from Internet Explorer, Firefox, or Chrome browser activities and/or history. In the figure below, I've selected at least one of each category to show what information IEF was able to discover:



#	URL	Potential Activity	Artifact	Artifact ID	Date/Time - (UTC) (MM/dd/yyyy)	Source
1	https://www.facebook.com/	At Facebook home page	Internet Explorer 10 Carved History	21	04/26/2013 02:33:10 AM	Windows 7.vmdk ...
317	https://www.facebook.com/	At Facebook home page	Chrome Web History	62	04/25/2013 01:17:03 AM	Windows 7.vmdk ...
397	https://www.facebook.com/	At Facebook home page	Firefox Web History	15	04/21/2013 07:46:40 PM	Windows 7.vmdk ...
271	https://www.facebook.com/login.php?login_attempt=1	Failed to log onto Facebook	Internet Explorer 10 History	405		Windows 7.vmdk ...
301	https://www.facebook.com/login.php?login_attempt=1	Failed to log onto Facebook	Chrome Web History	30	04/21/2013 07:45:43 PM	Windows 7.vmdk ...
57	https://www.facebook.com/groups/28802990461146 2/9	Looking at Facebook group with group id: 28802990461146 2	Browser Activity	1585		Windows 7.vmdk ...
235	http://www.facebook.com/places/map_iframe.php?locale=en_US&id=u_a_g&controller=a...	Looking at Facebook maps of profile id: places	Internet Explorer 10 History	341		Windows 7.vmdk ...
50	http://www.facebook.com/photo.php?fbid=10151342084301930&set=a.167899601929.1...	Looking at Facebook photo with id: 10151342084301930, album id: ...	Browser Activity	1575		Windows 7.vmdk ...
207	https://www.facebook.com/windowsseven.forensics	Looking at Facebook profile with profile id: windowsseven.forensics	Internet Explorer 10 History	165		Windows 7.vmdk ...
342	https://www.facebook.com/windowsseven.forensics	Looking at Facebook profile with profile id: windowsseven.forensics	Chrome Web History	174	05/02/2013 03:21:20 PM	Windows 7.vmdk ...
414	https://www.facebook.com/windowsseven.forensics	Looking at Facebook profile with profile id: windowsseven.forensics	Firefox Web History	95	05/03/2013 08:47:37 PM	Windows 7.vmdk ...
538	https://www.facebook.com/ajax/typeahead/search.php?value=Comment&context=topics...	Typing in search values: Comment	Browser Activity	3486		Windows 7.vmdk ...
544	https://www.facebook.com/ajax/typeahead/search.php?value=Daily&viewer=100005370...	Typing in search values: Daily	Browser Activity	3648		Windows 7.vmdk ...
820	https://www.facebook.com/ajax/typeahead/search.php?value=Post&viewer=1000053701...	Typing in search values: Post	Browser Activity	4182		Windows 7.vmdk ...
28	https://www.facebook.com/ajax/pagelet/generic.php/groupsnuxtourpagelet	Unknown	Browser Activity	1411		Windows 7.vmdk ...

Figure 33 Windows 7 Facebook URLs

In some cases, the URLs are still active and can be used to view what the user was looking at. In addition, we are also able to see some of the keyboard activity of the user in the form of the "Typing in search values:" Potential Activity. This would be especially useful to an investigator.

IEF Timeline

One of the really great features of IEF is its ability to create a timeline of activity for the artifacts that it's uncovered. Using the IEF Timeline application, an investigator can review the activities that took place on a given day, at a given time, and pertaining to specific aspects of Internet acitivity. For example, in the figure below, I've elected to see a timeline of Facebook URLs, Facebook Status Updates/Wall Posts/Comments, and Twitter from April 20th, 2013 to May 6th, 2013 (the time period in which the data generation process took place).

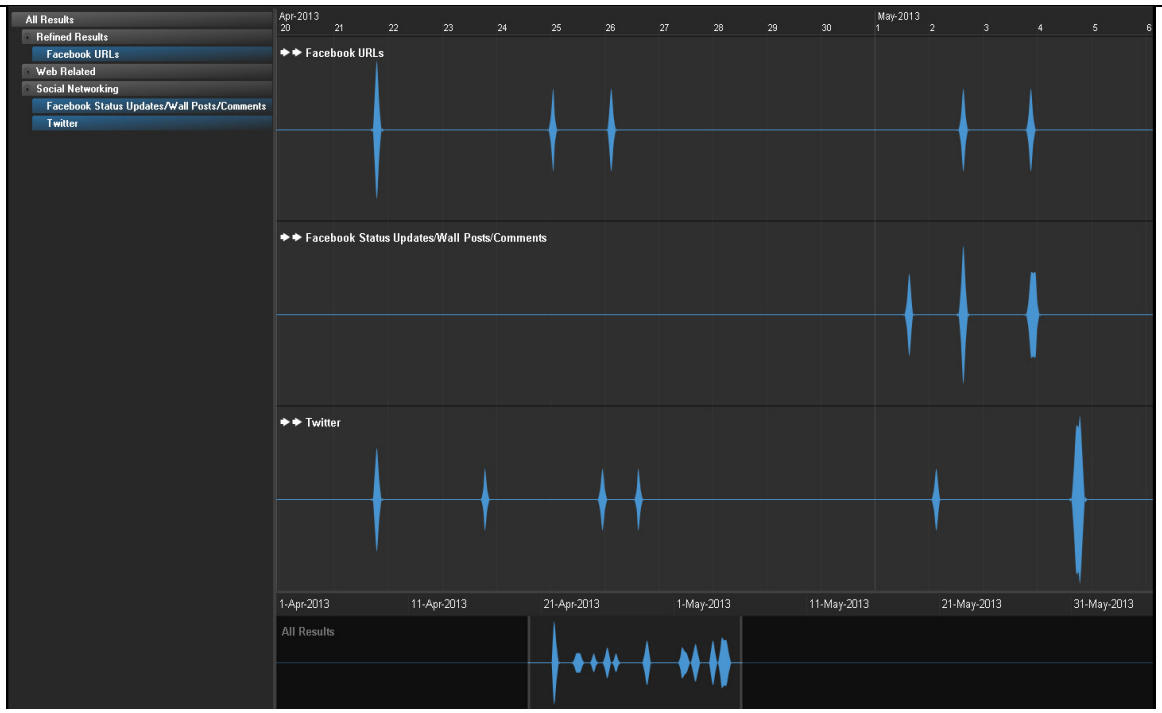


Figure 34 IEF Timeline for Social Media Items

From this timeline, I can then drill down into specific records for each of the different categories to find out what activities took place on a given day at a given time:

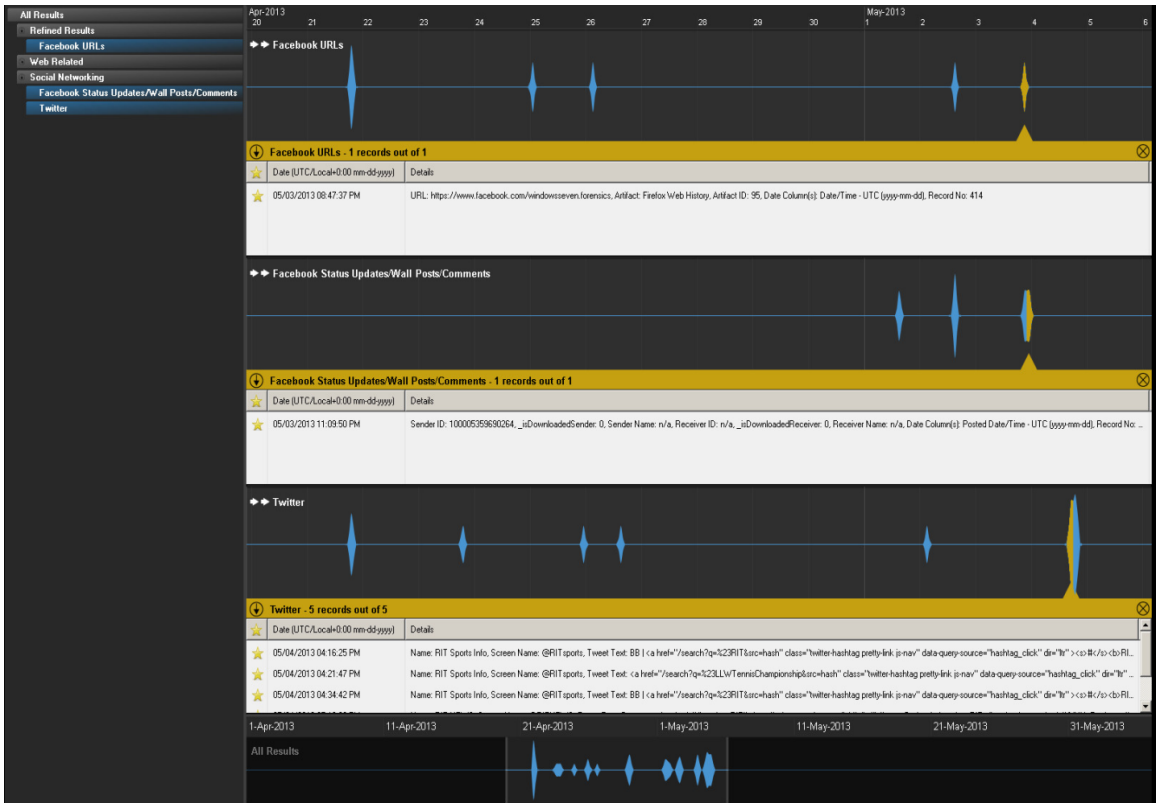


Figure 35 IEF Timeline for Social Media Items with Details

Email

Another set of artifacts that I worked on recovering were email artifacts. During the data generation process I sent and received many emails from both the Windows 7 Gmail and Live email accounts using Windows Live Mail 2012. Using FTK, and its ability to locate email items, I was able to recover the emails that I sent and received. FTK divided the emails based upon recipient email addresses, so I was able to view email that was received by the Windows 7 Gmail and Live accounts as well as email that was sent to the Windows 8 Gmail and Live accounts from the Windows 7 email accounts.

In the case of email sent to peterwilson.win7@gmail.com, FTK found a total of 90 emails. Most of these emails were from the accounts that I created for the purpose of data generation but a few others were from Facebook, Twiiter, or the email provider:

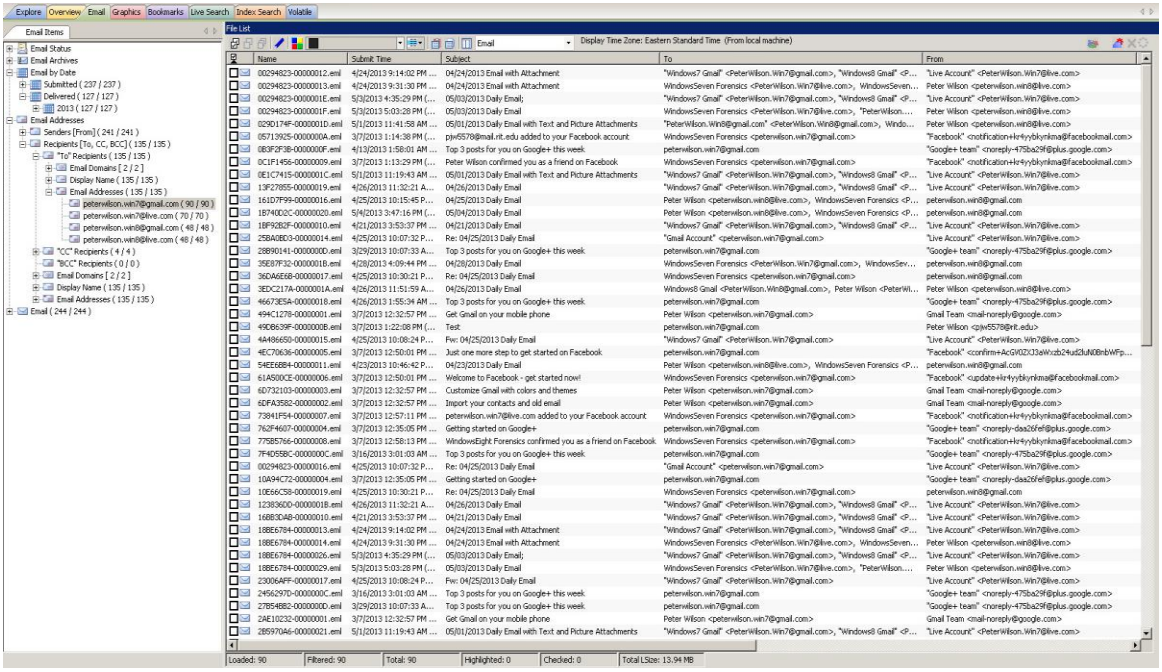


Figure 36 Email sent to peterwilson.win7@gmail.com

In the case of email sent to peterwilson.win7@live.com, FTK found a total of 70 emails. Most of these emails were from the accounts that I created for the purpose of data generation but a few others were from Facebook, Twiiter, or the email provider:

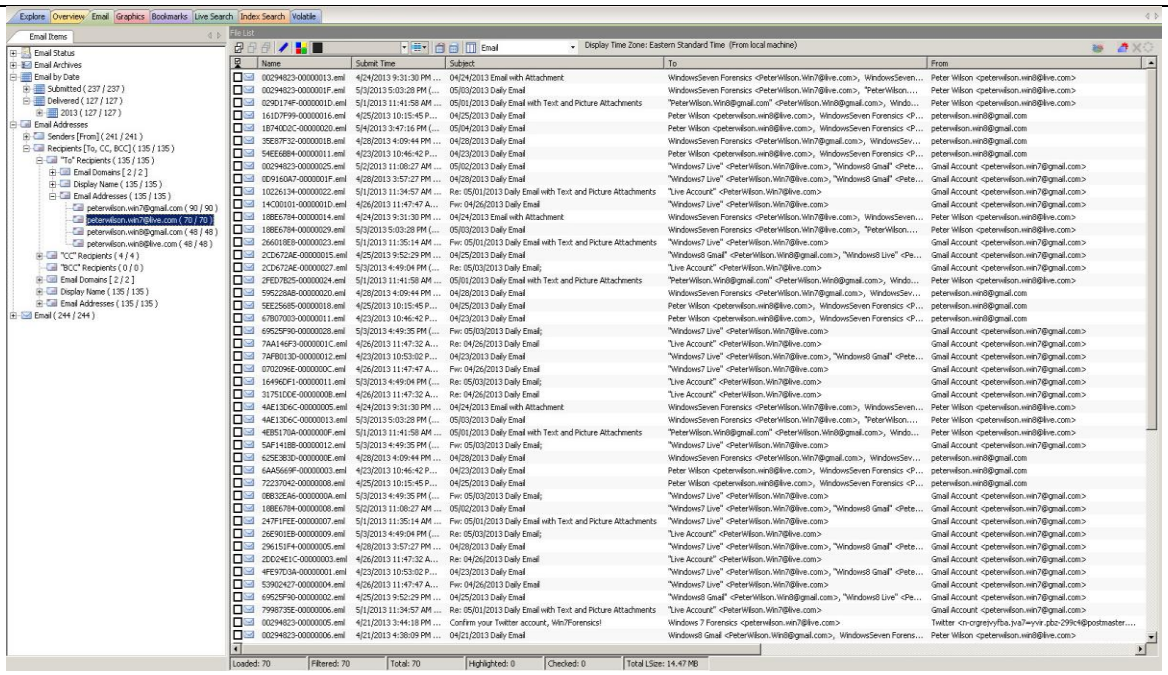


Figure 37 Email sent to peterwilson.win7@live.com

In the case of email sent from peterwilson.win7@gmail.com, FTK found a total of 35 emails. All of the emails sent from this accounts were sent to accounts that I created for the purpose of data generation:

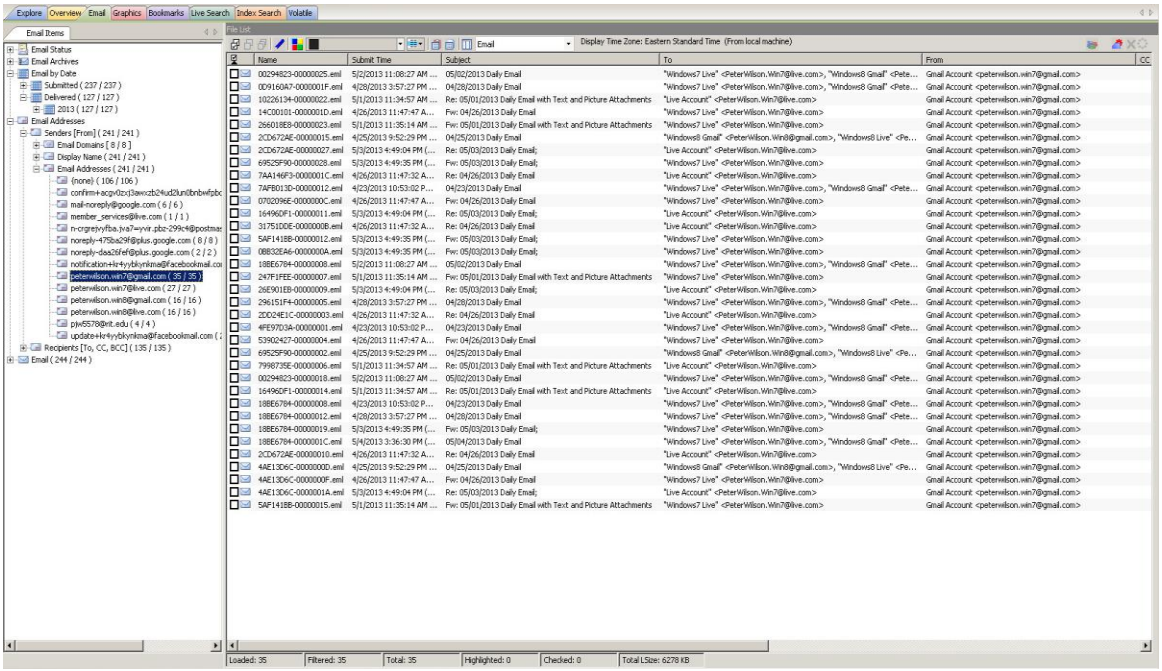


Figure 38 Email sent from peterwilson.win7@gmail.com

In the case of email sent from peterwilson.win7@;live.com, FTK found a total of 27 emails. All of the emails sent from this accounts were sent to accounts that I created for the purpose of data generation:

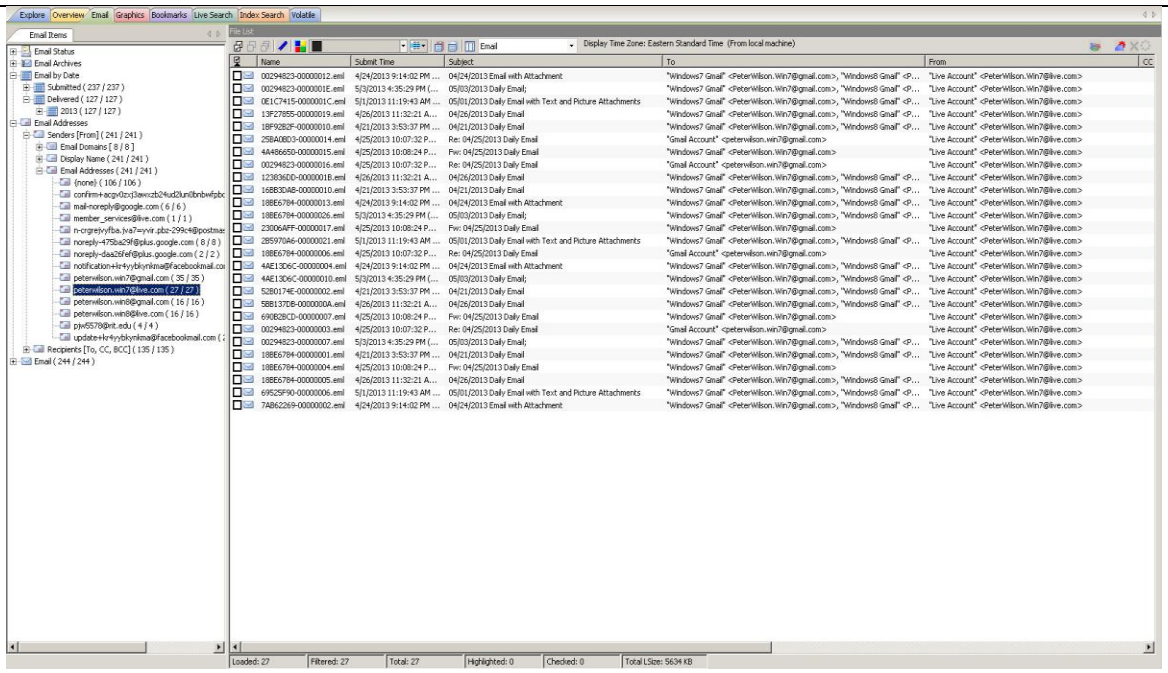


Figure 39 Email sent from peterwilson.win7@live.com

FTK found a total of 15 emails that were forwards of previously sent emails. In all of the emails, the receiver was either peterwilson.win7@gmial.com or peterwilson.win7@live.com:

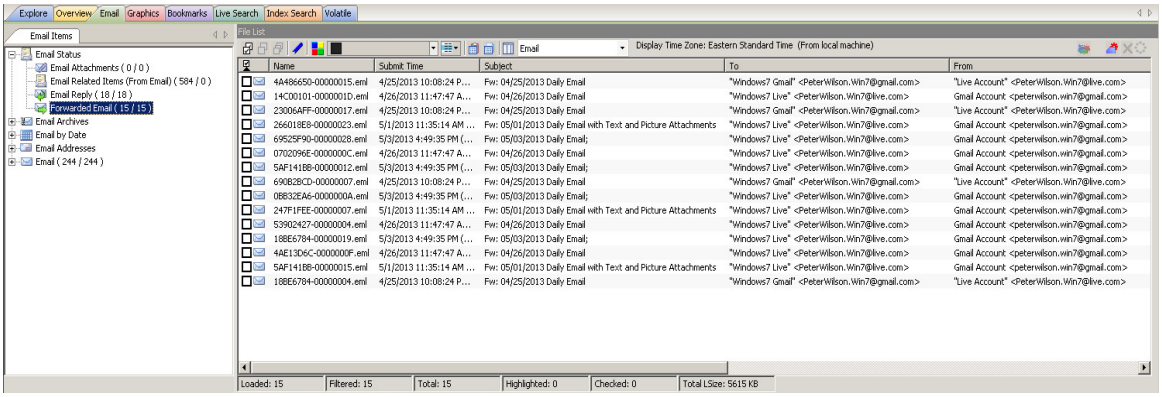


Figure 40 Forwarded Emails

FTK found a total of 18 emails that were replies to previously sent emails. In all of the emails, the receiver was either peterwilson.win7@gmial.com or peterwilson.win7@live.com:

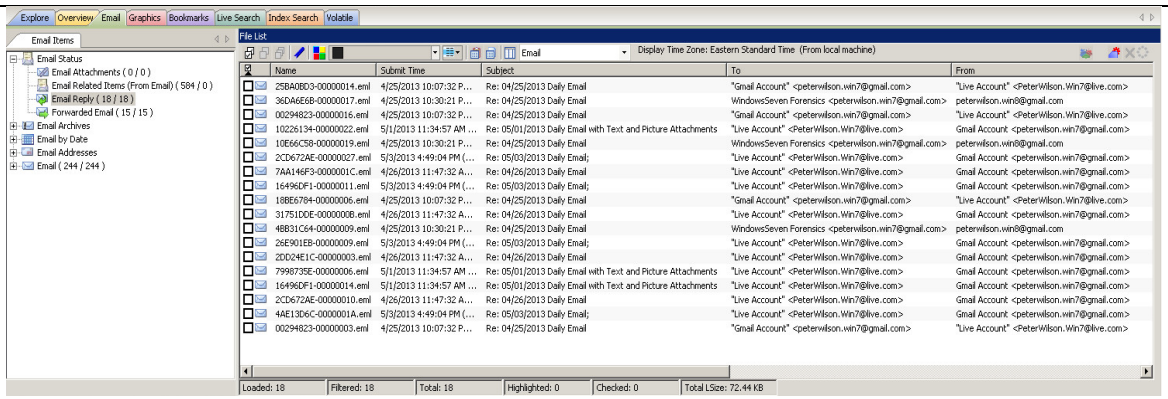


Figure 41 Replied Emails

FTK did not uncover any emails with attachments, despite the fact that I sent emails with attachments a total of four times throughout the data generation process. I am unsure as to why this is the case. When I view an email that would have had an attachment sent with it I see information pertaining to the attachment, but am unable to view the attachments themselves:

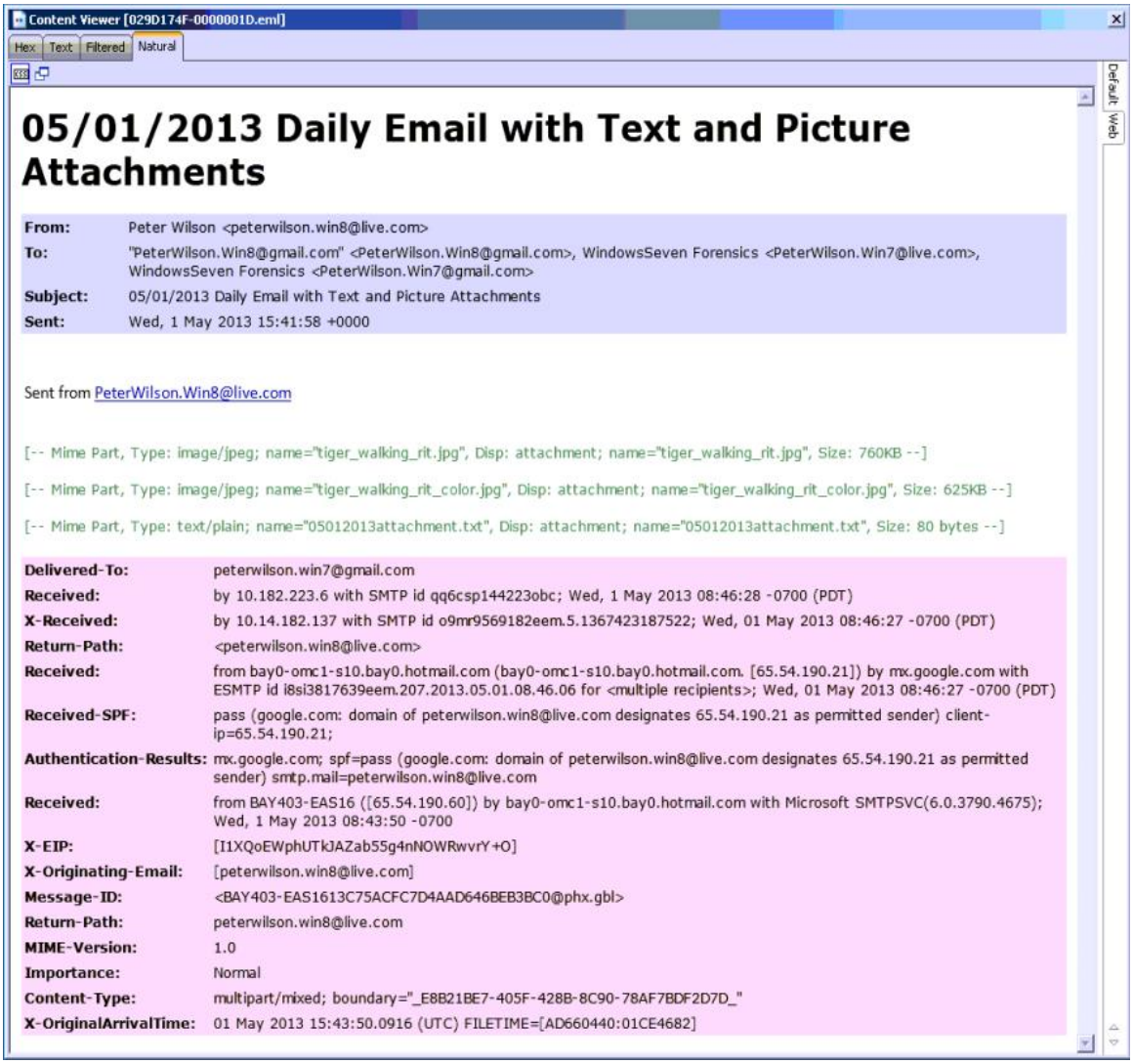


Figure 42 Recovered Email with Attachments

While I was unable to view the actual attachments with the emails that they were attached to, I was able to locate each of the files by doing a search using both EnCase and FTK.

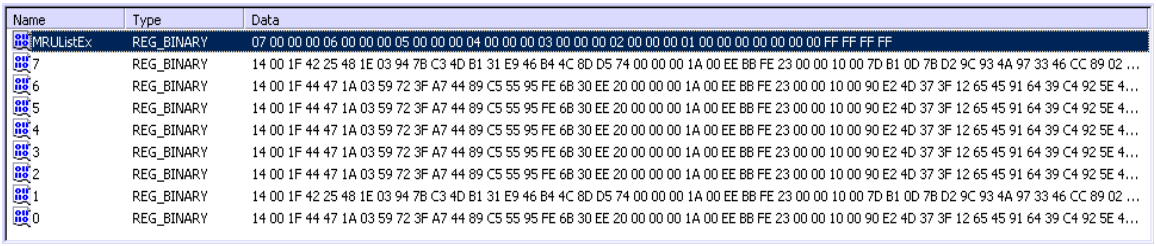
Registry

The Windows registry often contains a lot of information regarding a user's activity on a system. Using the AccessData Regsistry Viewer, along with an exported versions of the Windows 7 registry hives I was able to uncover several pieces of information that would be useful to a forensic investigator.

Windows 7 User Hive

The Windows 7 User hive (NTUSER.dat) found within the C:\Users\Windows7 directory as NTUSER.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 7 virtual machine.

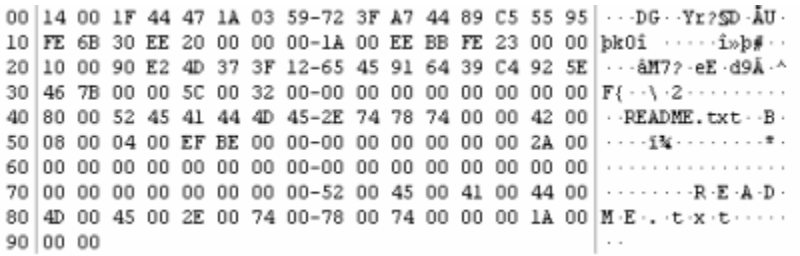
When we explore the registry key NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\ComDlg32\OpenSavePIDlMRU we are able to see a listing of files that have recently been opened or saved:



Name	Type	Data
MRUListEx	REG_BINARY	07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
7	REG_BINARY	14 00 1F 42 25 48 1E 03 94 7B C3 4D B1 31 E9 46 B4 4C 8D D5 74 00 00 00 1A 00 EE BB FE 23 00 00 10 00 7D B1 0D 7B D2 9C 93 4A 97 33 46 CC 89 02 ...
6	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 C4 92 5E 4...
5	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 C4 92 5E 4...
4	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 C4 92 5E 4...
3	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 C4 92 5E 4...
2	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 C4 92 5E 4...
1	REG_BINARY	14 00 1F 42 25 48 1E 03 94 7B C3 4D B1 31 E9 46 B4 4C 8D D5 74 00 00 00 1A 00 EE BB FE 23 00 00 10 00 7D B1 0D 7B D2 9C 93 4A 97 33 46 CC 89 02 ...
0	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 C4 92 5E 4...

Figure 43 OpenSavePIDlMRU Registry Key

While the data portion of the recently modified files appears in hexadecimal, the Registry Viewer has the ability to convert that into ASCII text. For example, when I select REG_BINARY 0, I can see both the hexadecimal data and ASCII data side by side:



```
00 14 00 1F 44 47 1A 03 59-72 3F A7 44 89 C5 55 95 ···DG·Yr?§D·ÅU·
10 FE 6B 30 EE 20 00 00 00-1A 00 EE BB FE 23 00 00 þk0î ·····î»þ#··
20 10 00 90 E2 4D 37 3F 12-65 45 91 64 39 C4 92 5E ···âM7?·eE·d9Ä·^
30 46 7B 00 00 5C 00 32 00-00 00 00 00 00 00 00 00 F{··\·2·········
40 80 00 52 45 41 44 4D 45-2E 74 78 74 00 00 42 00 ··README.txt··B·
50 08 00 04 00 EF BE 00 00-00 00 00 00 00 00 2A 00 ····ï¾·········*·
60 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
70 00 00 00 00 00 00 00 00-52 00 45 00 41 00 44 00 ········R·E·A·D·
80 4D 00 45 00 2E 00 74 00-78 00 74 00 00 00 1A 00 M·E·.·t·x·t·····
90 00 00                                           ··
```

Figure 44 HEX and ASCII Data REG_BINARY 0 OpenSavePIDIMRU

This is the case for every item within the OpenSavePIDIMRU. Using this ability I can see the most recently opened or saved files. From this we can see that the following names correspond to the following applications:

Table 11 OpenSavePIDIMRU Applications

Name	Application in Text
7	05012013attachment.txt.txt
6	Rit_alum_assoc.jpg

5	Tiger_walking_rit_color.jpg
4	Tiger_walking.jpg
3	Rit_white_no_bar.jpg
2	Rit_black_no_bar.jpg
1	04262013daily.txt
0	README.txt

When we explore the registry key NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\ComDlg32\LastVisitedMRU we are able to see a listing of applications that were recently used to open or save the files listed in the OpenSavePIDIMRU registry key:

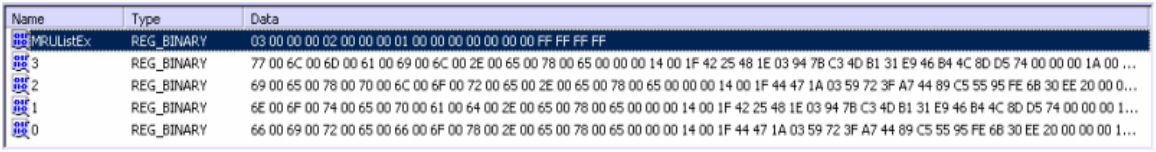


Figure 45 LastVisitedPidMRU Registry Key

As was the case with the previous registry key, the data portion appears in hexadecimal but Registry Viewer can convert that into ASCII text:

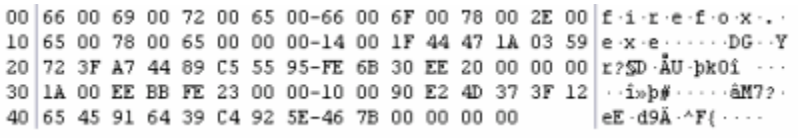


Figure 46 HEX and ASCII Data REG_BINARY 0 LastVisitedMRU

From this we can see that the following names correspond to the following applications:

Table 12 LastVisitedPidMRU Applications

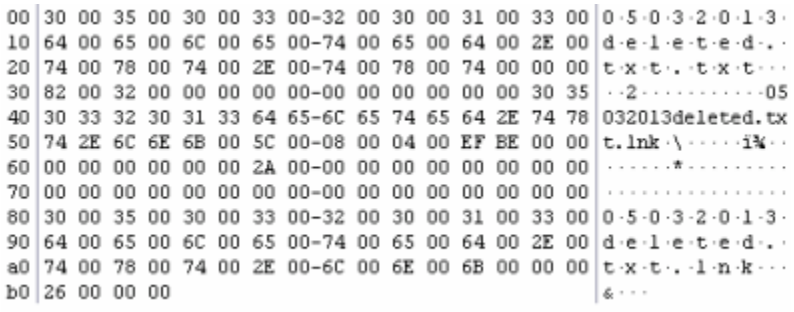
Name	Application in Text
3	Wlmail.exe
2	Iexplore.exe
1	Notepad.exe
0	Firefox.exe

When we explore the registry key NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\RecentDocs we are able to see a listing of files and folders that were recently opened:

Name	Type	Data
MRUListEx	REG_BINARY	05 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 11 00 00 00 10 00 00 00 02 00 00 00 0F 00 00 00 04 00 00 00 0E 00 00 00 0D 00 00 00 0C 00 00 00 0B...
5	REG_BINARY	30 00 35 00 30 00 34 00 30 00 31 00 33 00 64 00 61 00 69 00 6C 00 79 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 7A 00 32 00 00 00 00...
0	REG_BINARY	30 00 35 00 30 00 33 00 32 00 30 00 31 00 33 00 64 00 65 00 6C 00 65 00 74 00 65 00 64 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 82...
1	REG_BINARY	30 00 35 00 30 00 33 00 32 00 30 00 31 00 33 00 61 00 74 00 74 00 61 00 63 00 68 00 6D 00 65 00 6E 00 74 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78...
3	REG_BINARY	30 00 35 00 30 00 33 00 32 00 30 00 31 00 33 00 64 00 61 00 69 00 6C 00 79 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 7C 00 32 00 00...
17	REG_BINARY	30 00 35 00 30 00 32 00 32 00 30 00 31 00 33 00 64 00 61 00 69 00 6C 00 79 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 7C 00 32 00 00...
16	REG_BINARY	30 00 35 00 30 00 31 00 32 00 30 00 31 00 33 00 64 00 65 00 6C 00 65 00 74 00 65 00 64 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 82...
2	REG_BINARY	30 00 35 00 30 00 31 00 32 00 30 00 31 00 33 00 61 00 74 00 74 00 61 00 63 00 68 00 6D 00 65 00 6E 00 74 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78...
15	REG_BINARY	30 00 35 00 30 00 31 00 32 00 30 00 31 00 33 00 64 00 61 00 69 00 6C 00 79 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 7C 00 32 00 00...
4	REG_BINARY	44 00 6F 00 77 00 6E 00 6C 00 6F 00 61 00 64 00 73 00 00 00 64 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 44 6F 77 6E 6C 6F 61 64 73 2E 6C 6E 6B 00 4...
14	REG_BINARY	72 00 69 00 74 00 5F 00 61 00 6C 00 75 00 6D 00 5F 00 61 00 73 00 73 00 6F 00 63 00 2E 00 6A 00 70 00 67 00 00 00 74 00 32 00 00 00 00 00 00 00 0...
13	REG_BINARY	74 00 69 00 67 00 65 00 72 00 5F 00 77 00 61 00 6C 00 6B 00 69 00 6E 00 67 00 5F 00 72 00 69 00 74 00 5F 00 63 00 6F 00 6C 00 6F 00 72 00 2E 00 6...
12	REG_BINARY	74 00 69 00 67 00 65 00 72 00 5F 00 77 00 61 00 6C 00 6B 00 69 00 6E 00 67 00 5F 00 72 00 69 00 74 00 2E 00 6A 00 70 00 67 00 00 00 7C 00 32 00 0...
11	REG_BINARY	72 00 69 00 74 00 5F 00 77 00 68 00 69 00 74 00 65 00 5F 00 6E 00 6F 00 5F 00 62 00 61 00 72 00 2E 00 6A 00 70 00 67 00 00 00 7A 00 32 00 00 00 00...
10	REG_BINARY	72 00 69 00 74 00 5F 00 62 00 6C 00 61 00 63 00 6B 00 5F 00 6E 00 6F 00 5F 00 62 00 61 00 72 00 2E 00 6A 00 70 00 67 00 00 00 7A 00 32 00 00 00 0...
9	REG_BINARY	30 00 34 00 32 00 38 00 32 00 30 00 31 00 33 00 64 00 65 00 6C 00 65 00 74 00 65 00 64 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 82...
8	REG_BINARY	30 00 34 00 32 00 38 00 32 00 30 00 31 00 33 00 64 00 61 00 69 00 6C 00 79 00 2E 00 74 00 78 00 74 00 2E 00 74 00 78 00 74 00 00 00 7C 00 32 00 00...
7	REG_BINARY	44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 00 00 64 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 44 6F 63 75 6D 65 6E 74 73 2E 6C 6E 6B 00 4...

Figure 47 RecentDocs Registry Key

As was the case with the previous registry key, the data portion appears in hexadecimal but Registry Viewer can convert that into ASCII text:



00	30 00 35 00 30 00 33 00-32 00 30 00 31 00 33 00	0·5·0·3·2·0·1·3·
10	64 00 65 00 6C 00 65 00-74 00 65 00 64 00 2E 00	d·e·l·e·t·e·d·.·
20	74 00 78 00 74 00 2E 00-74 00 78 00 74 00 00 00	t·x·t·.·t·x·t···
30	82 00 32 00 00 00 00 00-00 00 00 00 00 00 30 35	··2···········05
40	30 33 32 30 31 33 64 65-6C 65 74 65 64 2E 74 78	032013deleted.tx
50	74 2E 6C 6E 6B 00 5C 00-08 00 04 00 EF BE 00 00	t.lnk·\·····i¾··
60	00 00 00 00 00 00 2A 00-00 00 00 00 00 00 00 00	·····*··········
70	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00	················
80	30 00 35 00 30 00 33 00-32 00 30 00 31 00 33 00	0·5·0·3·2·0·1·3·
90	64 00 65 00 6C 00 65 00-74 00 65 00 64 00 2E 00	d·e·l·e·t·e·d·.·
a0	74 00 78 00 74 00 2E 00-6C 00 6E 00 6B 00 00 00	t·x·t·.·l·n·k···
b0	26 00 00 00	&···

Figure 48 HEX and ASCII Data REG_BINARY 0 RecentDocs Registry Key

From this we can see that the following names correspond to the following applications:

Table 13 RecentDocs Applications

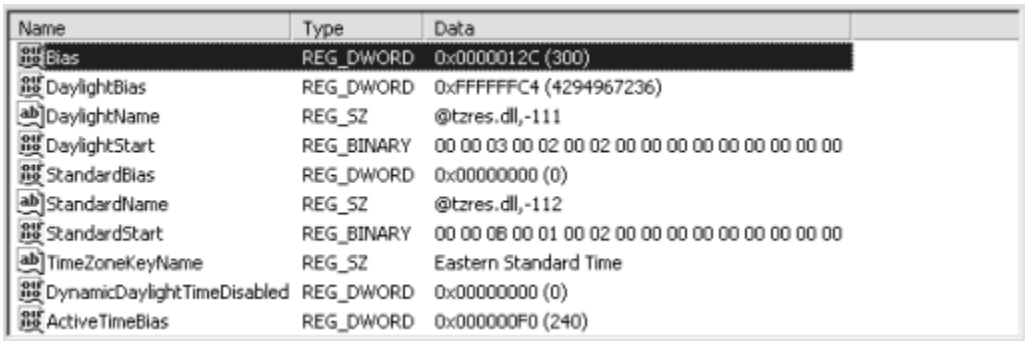
Name	Application in Text
15	05012013attachment.txt.lnk
14	Rit_alum_assoc.lnk
13	Tiger_walking_rit_color.lnk
12	Tiger_walking.lnk
11	Rit_white_no_bar.lnk
10	Rit_black_no_bar.lnk
9	04282013deleted.txt.lnk
8	04282013daily.txt.lnk
7	Documents.lnk
5	05032013daily.txt.lnk
4	Downbloads.lnk
3	05032013daily.txt.lnk

2	05012013attachment.txt.lnk
1	05032013attachment.txt.lnk
0	05032013deleted.txt.lnk

System Hive

The Windows 7 System hive (SYSTEM.dat) found within the C:\Windows\System32\ Config directory as SYSTEM.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 7 virtual machine.

When we explore the registry key SYSTEM.dat\ControlSet002\Control\TimeZoneInfo rmation we are able to see information pertaining to the time zone of the Windows 7 virtual machine. This information is especially useful to forensic investigators as all timestamps within files on this computer are based off of this information:



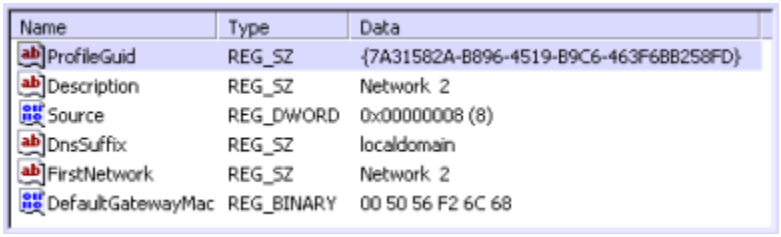
Name	Type	Data
Bias	REG_DWORD	0x0000012C (300)
DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000000F0 (240)

Figure 49 TimeZoneInformation Registry Key

Software

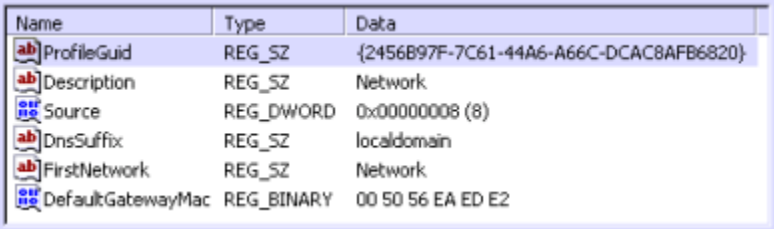
The Windows 7 Software hive (SOFTWARE.dat) found within the C:\Windows\System 32\Config directory as SOFTWARE.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 7 virtual machine.

When we explore the registry key SOFTWARE.dat\ Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged we are able to see information pertaining to the network history of the Windows 7 virtual machine:



Name	Type	Data
ProfileGuid	REG_SZ	{7A31582A-B896-4519-B9C6-463F6BB258FD}
Description	REG_SZ	Network 2
Source	REG_DWORD	0x00000008 (8)
DnsSuffix	REG_SZ	localdomain
FirstNetwork	REG_SZ	Network 2
DefaultGatewayMac	REG_BINARY	00 50 56 F2 6C 68

Figure 50 Unmanaged Network 2 Registry Key



Name	Type	Data
ProfileGuid	REG_SZ	{2456B97F-7C61-44A6-A66C-DCAC8AFB6820}
Description	REG_SZ	Network
Source	REG_DWORD	0x00000008 (8)
DnsSuffix	REG_SZ	localdomain
FirstNetwork	REG_SZ	Network
DefaultGatewayMac	REG_BINARY	00 50 56 EA ED E2

Figure 51 Unmanaged Network Registry Key

From this we can identify networks that the virtual machine has been connected to. We can also identify important details such as domain name, SSID, and gateway MAC address.

In addition to the Unmanaged registry key, there are additional registry keys that also contain information about network history. In the case of the Windows 7 virtual machine, these keys had no information: SOFTWARE.dat\Microsoft\Windows NT\CurrentVersion\NetworkList \Signatures\Managed, SOFTWARE.dat\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla \Cache.

SAM

The Windows 7 Security Accounts Manager (SAM) hive (SAM.dat) found within the C:\Windows\System32\Config directory as SAM.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 7 virtual machine.

When we explore the registry key SAM.dat\Domains\Accounts\Users we are able to see a listing of the users that exist on the Windows 7 virtual machine including the administrator, guest, and Windows7 accounts. From this key we can see quite a bit of useful information relating to this user. Information like last logon time, last password change time, invalid logon count, last failed logon time, and many others:

Key Properties	
Last Written Time	5/3/2013 14:09:12 UTC
SID unique identifier	1000
User Name	Windows7
Logon Count	16
Last Logon Time	5/3/2013 14:09:12 UTC
Last Password Change Time	3/7/2013 19:18:41 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	false
Country Code	1 (United States)
Hours Allowed	Anytime
Has LAN Manager Password	false
Has NTLMv2 Password	true

Figure 52 Users Registry Key

Conclusion

This document explores forensic artifacts including creation/deletion, web browsing, social media, email and the Windows registry. Using both FTK and EnCase, I was able to uncover a majority of the user data that was

generated. This serves as a detailed report of the forensic findings made while examining the Windows 7 virtual machine to be included within the appendix of my thesis and later used in a forensic comparison of Windows 7 and Windows 8.

Appendix C: Windows 8 Forensic Report

Windows 8 Forensic Report

07/20/2013

Introduction

This document serves as a detailed report of the forensic findings made while examining the Windows 8 virtual machine. Using both FTK and EnCase, I was able to uncover a majority of the user data that was generated. This report specifically looks at a number of different forensic artifacts including file creation/deletion, web browsing, social media, email and registry.

File Creation/Deletion

The first artifacts that I set out to discover were any artifacts pertaining to user file creation or deletion. In Windows 8, like Windows 7, the majority of user files are stored within the C:\Users\ directory, which contains several subfolders for each created user. Given that the user I created is Windows8, I primarily looked in the Windows8 subfolder. This directory includes folders for Contacts, Desktop, Downloads, Favorites, Links, Documents, Music, Pictures, Videos, and several other folders.

While exploring the folders within the Windows7 user directory I was able to uncover several relevant artifacts. First, I was able to easily find many of the daily and attachment files that I created using FTK, though it is interesting to note that in some cases the files have a double extension, as was the case with Windows 7:

Name	E...	Created	Accessed	Modified	Path	P-Size	L-Size
$I30		3/7/2013 11:54:25 PM (...	5/4/2013 3:46:02 PM (...	5/4/2013 3:46:02 PM (2...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/$I30	4096 B	4096 B
04232013Daily.txt	txt	4/23/2013 10:45:38 PM...	4/23/2013 10:45:39 PM...	4/23/2013 10:46:03 PM...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/04232013Daily.txt	44 B	44 B
04242013attachment.txt	txt	4/24/2013 9:30:38 PM (...	4/24/2013 9:30:39 PM ...	4/24/2013 9:30:39 PM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/04242013attachment.txt	57 B	57 B
04252013Daily.txt	txt	4/25/2013 10:14:47 PM...	4/25/2013 10:14:47 PM...	4/25/2013 10:14:48 PM...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/04252013Daily.txt	43 B	43 B
04262013Daily.txt	txt	4/26/2013 11:50:48 AM...	4/26/2013 11:50:48 A...	4/26/2013 11:51:18 AM...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/04262013Daily.txt	46 B	46 B
04282013Daily.txt	txt	4/28/2013 4:08:07 PM (...	4/28/2013 4:08:07 PM ...	4/28/2013 4:08:07 PM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/04282013Daily.txt	45 B	45 B
05012013attachment.txt	txt	5/1/2013 11:41:11 AM ...	5/1/2013 11:41:11 AM ...	5/1/2013 11:41:11 AM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/05012013attachment.txt	80 B	80 B
05012013Daily.txt	txt	5/1/2013 11:40:03 AM ...	5/1/2013 11:40:03 AM ...	5/1/2013 11:40:03 AM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/05012013Daily.txt	46 B	46 B
05022013Daily.txt.txt	txt	5/2/2013 11:26:38 AM ...	5/2/2013 11:26:38 AM ...	5/2/2013 11:27:00 AM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/05022013Daily.txt.txt	46 B	46 B
05032013attachment.txt	txt	5/3/2013 4:59:41 PM (2...	5/3/2013 4:59:41 PM (...	5/3/2013 4:59:41 PM (2...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/05032013attachment.txt	80 B	80 B
05032013daily,txt.txt	txt	5/3/2013 4:58:52 PM (2...	5/3/2013 4:58:52 PM (...	5/3/2013 4:58:52 PM (2...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/05032013daily,txt.txt	45 B	45 B
05042013daily,txt.txt	txt	5/4/2013 3:46:02 PM (2...	5/4/2013 3:46:02 PM (...	5/4/2013 3:46:07 PM (2...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/05042013daily,txt.txt	45 B	45 B
desktop.ini	ini	3/7/2013 11:56:39 PM (...	3/7/2013 11:56:39 PM ...	4/14/2013 4:11:10 AM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/desktop.ini	402 B	402 B
My Music		3/7/2013 11:54:26 PM (...	3/7/2013 11:54:26 PM ...	3/7/2013 11:54:26 PM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/My Music	120 B	120 B
My Pictures		3/7/2013 11:54:26 PM (...	3/7/2013 11:54:26 PM ...	3/7/2013 11:54:26 PM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/My Pictures	132 B	132 B
My Videos		3/7/2013 11:54:26 PM (...	3/7/2013 11:54:26 PM ...	3/7/2013 11:54:26 PM (...	Windows 8-flat.vmdk/Partition 1/NONAME [NTFS]/[root]/Users/Windows8/Documents/My Videos	124 B	124 B

Figure 53 Windows 8 Created Documents

When I viewed the contents of the files, they simply contained whatever text I had placed into them when I first created them during the data generation process:

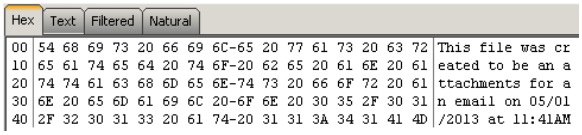


Figure 54 Windows 8 Created File

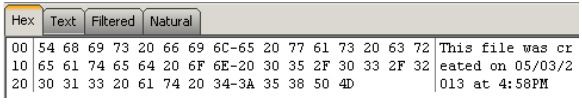


Figure 55 Windows 8 Created File

Using EnCase and its evidence processor, I managed to recover a few of the files that I had deleted using

EnCase. As was the case with Windows 7, the process was very arduous as I had to manually search through all of the recovered files and folders. It took me longer to find deleted files than it did for Windows 7 because of the manual nature of the task. Still, I was able to find the file that I deleted on 04/28/2013 along with a reference to the original file location:

Name	Logical Size	Last Accessed	File Created	Last Written	Signature Analysis	File Type	Item Path
$RFGBREV.txt	83	04/28/13 04:31:08PM	04/28/13 04:08:13PM	04/28/13 04:08:13PM	Match	Text	Windows 8-flat\C\Recovered Folders\\$Recycle.Bin\S-1-5-21-1414118115-6188285350-108115063
$IFGBREV.txt	545	04/28/13 04:51:51PM	04/28/13 04:24:51PM	04/28/13 04:24:51PM	Alias	Enhanced Metafile Graphic	Windows 7-flat\C\Recovered Folders\\$Recycle.Bin\S-1-5-21-1414118115-6188285350-108115063

Figure 56 Windows 8 Recovered Deleted Files

The first file, $RFGBREV.txt had the following contents:

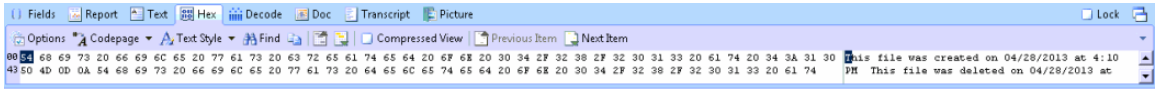


Figure 57 Recovered File $RFGBREV.txt

The second file, $IFGBREV.txt has the following contents:

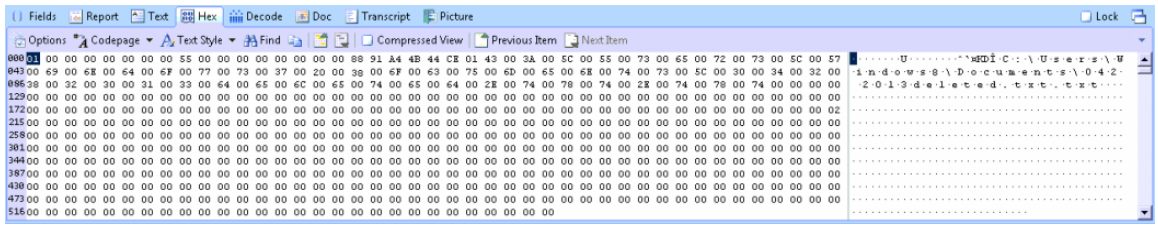


Figure 58 Recovered File $IFGBREV.txt

As was the case with Windows 7, I attempted to run several other searches on both Lost Files and Recovered Folders and ended up with 218 results when I searched for the keyword “deleted”. When I sifted through the entire search results I was only able to find that the previously uncovered $RFGBREV.txt were files that I had deleted.

Web Browsing (Internet Explorer, Firefox, Chrome)

The second set of artifacts that I set out to uncover were web browsing artifacts. In the case of the Windows 8 virtual machine, Internet Explorer, the Internet Explorer App, Firefox and Chrome were the web browsers that I used to generate data. So, for each of the browsers I examined Internet history, downloads, favorites, and other temporary Internet files. Using EnCase and its records processor I was able to quickly uncover web browsing artifacts for all three browsers.

Internet Explorer and Internet Explorer App

Uncovering information regarding web browsing with Internet Explorer and with the Internet Explorer Appwas relatively simple. Using the EnCase records processor I was able to easily view the history, and favorites. In the case of browsing history, EnCase examined the TypedURLs registry key within the Windows registry. This entry can be found within HKEY_CURRENT_User\Software\Microsoft\Internet Explorer\TypedURLs and thereby making it specific to the currently logged on user, in our case Windows 8. From the TypedURLs key, I was able to see a total of the twenty eight most recently viewed web pages, though it appears that they repeat after only fourteen:

	Browser Type	Title	Last Modification Time	Url Name	Profile Name	Internet Artifact Type
1	Internet Explorer (Windows)	url1	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49984&source=enewsletter	Windows8	History\Typed URL
2	Internet Explorer (Windows)	url2	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49981&source=enewsletter	Windows8	History\Typed URL
3	Internet Explorer (Windows)	url3	05/02/13 11:30:07AM	http://mirrors.rit.edu/	Windows8	History\Typed URL
4	Internet Explorer (Windows)	url4	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49976&source=enewsletter	Windows8	History\Typed URL
5	Internet Explorer (Windows)	url5	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49956&source=enewsletter	Windows8	History\Typed URL
6	Internet Explorer (Windows)	url6	05/02/13 11:30:07AM	http://google.com/	Windows8	History\Typed URL
7	Internet Explorer (Windows)	url7	05/02/13 11:30:07AM	http://mirrors.rit.edu/centos/6.4/isos/i386/CentOS-6.5-i386-netinstall.iso	Windows8	History\Typed URL
8	Internet Explorer (Windows)	url8	05/02/13 11:30:07AM	http://live.com/	Windows8	History\Typed URL
9	Internet Explorer (Windows)	url9	05/02/13 11:30:07AM	http://gmail.com/	Windows8	History\Typed URL
10	Internet Explorer (Windows)	url10	05/02/13 11:30:07AM	http://twitter.com/	Windows8	History\Typed URL
11	Internet Explorer (Windows)	url11	05/02/13 11:30:07AM	http://facebook.com/	Windows8	History\Typed URL
12	Internet Explorer (Windows)	url12	05/02/13 11:30:07AM	http://www.rit.edu/news/nandedaily.php	Windows8	History\Typed URL
13	Internet Explorer (Windows)	url13	05/02/13 11:30:07AM	http://en.wikipedia.org/wiki/Main_Page	Windows8	History\Typed URL
14	Internet Explorer (Windows)	url14	05/02/13 11:30:07AM	http://go.microsoft.com/fwlink/p/?LinkId=255141	Windows8	History\Typed URL
15	Internet Explorer (Windows)	url1	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49984&source=enewsletter		History\Typed URL
16	Internet Explorer (Windows)	url2	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49981&source=enewsletter		History\Typed URL
17	Internet Explorer (Windows)	url3	05/02/13 11:30:07AM	http://mirrors.rit.edu/		History\Typed URL
18	Internet Explorer (Windows)	url4	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49976&source=enewsletter		History\Typed URL
19	Internet Explorer (Windows)	url5	05/02/13 11:30:07AM	http://www.rit.edu/news/story.php?id=49956&source=enewsletter		History\Typed URL
20	Internet Explorer (Windows)	url6	05/02/13 11:30:07AM	http://google.com/		History\Typed URL
21	Internet Explorer (Windows)	url7	05/02/13 11:30:07AM	http://mirrors.rit.edu/centos/6.4/isos/i386/CentOS-6.5-i386-netinstall.iso		History\Typed URL
22	Internet Explorer (Windows)	url8	05/02/13 11:30:07AM	http://live.com/		History\Typed URL
23	Internet Explorer (Windows)	url9	05/02/13 11:30:07AM	http://gmail.com/		History\Typed URL
24	Internet Explorer (Windows)	url10	05/02/13 11:30:07AM	http://twitter.com/		History\Typed URL
25	Internet Explorer (Windows)	url11	05/02/13 11:30:07AM	http://facebook.com/		History\Typed URL
26	Internet Explorer (Windows)	url12	05/02/13 11:30:07AM	http://www.rit.edu/news/nandedaily.php		History\Typed URL
27	Internet Explorer (Windows)	url13	05/02/13 11:30:07AM	http://en.wikipedia.org/wiki/Main_Page		History\Typed URL
28	Internet Explorer (Windows)	url14	05/02/13 11:30:07AM	http://go.microsoft.com/fwlink/p/?LinkId=255141		History\Typed URL

Figure 59 Internet Explorer and Internet Explorer App History

In addition to web browsing history, the records processor was able to uncover information regarding Internet Explorer bookmarks. During the data generation process I setup bookmarks within Internet Explorer for Live Email, Gmail, Twitter, Facebook, RIT News, and Wikipedia. This is confirmed by the fact that the records processor was able to find these exact bookmarks, in addition to a few extras that existed by default:

Browser Type	Created	Title	Url Name	Profile Name	Internet Artifact Type
Internet Explorer (Windows)	06/02/12 10:47:08AM	Read Me	http://go.microsoft.com/fwlink/?LinkId=129765		Bookmarks
Internet Explorer (Windows)	06/02/12 10:47:08AM	Read Me	http://go.microsoft.com/fwlink/?LinkId=129765		Bookmarks
Internet Explorer (Windows)	04/21/13 04:25:33PM	Twitter	https://twitter.com/	Windows8	Bookmarks
Internet Explorer (Windows)	03/07/13 11:56:36PM	Bing	http://go.microsoft.com/fwlink/p/?LinkId=255142		Bookmarks
Internet Explorer (Windows)	04/21/13 04:07:54PM	Twitter	https://twitter.com/	Windows8	Bookmarks
Internet Explorer (Windows)	04/21/13 04:07:42PM	Welcome to Facebook - Log In, Sign Up or Learn More	https://www.facebook.com/	Windows8	Bookmarks
Internet Explorer (Windows)	04/21/13 04:07:10PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows8	Bookmarks
Internet Explorer (Windows)	04/21/13 04:06:55PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows8	Bookmarks
Internet Explorer (Windows)	04/21/13 04:08:03PM	gmail Email from Google	https://accounts.google.com/ServiceLogin?service=mail&passive=true...	Windows8	Bookmarks
Internet Explorer (Windows)	04/21/13 04:08:11PM	Live Email Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1366574...	Windows8	Bookmarks

Figure 60 Internet Explorer and Internet Explorer App Bookmarks

When I attempted to view what EnCase uncovered for Internet Explorer's and the Internet Explorer App's Temporary Internet Files and Internet Cache I was surprised to find no items. Unlike Windows 7, EnCase was unable to recover the cache and temporary internet files from the browsers.

Firefox

Uncovering information pertaining to the history, favorites, and cache of Firefox was just as simple as it was with Internet Explorer and the Internet Explorer App. However, instead of looking to a registry key, EnCase examined Firefox's sqlite databases located within user profiles. In this case, that location is C:\Users\Windows 8\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite. From these databases we are able

to recover a complete browsing history for the Firefox browser. Unfortunately, EnCase was unable to display the time at which specific website were visited, but we can see that Facebook, Twitter, RIT News, Wikipedia, and other websites were visited during the data generation process using Firefox:

Browser Type	Title	Url Name	Profile Name	Internet Artifact Type
Mozilla 3 (Windows/Mac)	MSN	http://t.msn.com/	Windows8	History
Mozilla 3 (Windows/Mac)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows8	History
Mozilla 3 (Windows/Mac)	Google	http://www.google.com/	Windows8	History
Mozilla 3 (Windows/Mac)	Chrome Browser	https://www.google.com/intl/en/chrome/browser...	Windows8	History
Mozilla 3 (Windows/Mac)	Chrome Browser	https://www.google.com/intl/en/chrome/browser...	Windows8	History
Mozilla 3 (Windows/Mac)	Sign in to your Microsoft account	https://login.live.com/ppsecure/post.srf?uiflavor=...	Windows8	History
Mozilla 3 (Windows/Mac)	Sign In	https://login.live.com/login.srf?wa=wsignin1.0&r...	Windows8	History
Mozilla 3 (Windows/Mac)	Sign in to your Microsoft account	https://login.live.com/ppsecure/InlineLogin.srf?ui...	Windows8	History
Mozilla 3 (Windows/Mac)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows8	History
Mozilla 3 (Windows/Mac)	Mozilla Firefox Web Browser — Free Download — mozilla.org	http://www.mozilla.org/en-US/firefox/new/	Windows8	History
Mozilla 3 (Windows/Mac)	Gmail: Email from Google	https://accounts.google.com/ServiceLogin?service...	Windows8	History
Mozilla 3 (Windows/Mac)	Facebook	https://www.facebook.com/	Windows8	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	Windows8	History
Mozilla 3 (Windows/Mac)		http://www.mozilla.com/en-US/firefox/20.0.1/first...	Windows8	History
Mozilla 3 (Windows/Mac)	Welcome to Firefox	http://www.mozilla.org/en-US/firefox/20.0.1/firstr...	Windows8	History
Mozilla 3 (Windows/Mac)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows8	History
Mozilla 3 (Windows/Mac)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows8	History
Mozilla 3 (Windows/Mac)	Facebook	https://www.facebook.com/	Windows8	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	Windows8	History
Mozilla 3 (Windows/Mac)	Reginald Heber - Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Reginald_Heber	Windows8	History
Mozilla 3 (Windows/Mac)	RIT screening of award-winning film 'United in Anger' debuts April 25 - RIT News	http://www.rit.edu/news/story.php?id=49951&so...	Windows8	History
Mozilla 3 (Windows/Mac)	Pollution Prevention Institute recognizes Brooklyn Navy Yard for environmental efforts - RIT News	http://www.rit.edu/news/story.php?id=49953&so...	Windows8	History
Mozilla 3 (Windows/Mac)	(16) Facebook	https://www.facebook.com/?sk=welcome	Windows8	History
Mozilla 3 (Windows/Mac)	Twitter	https://twitter.com/	Windows8	History
Mozilla 3 (Windows/Mac)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows8	History
Mozilla 3 (Windows/Mac)	Alcohol laws of New Jersey - Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Alcohol_laws_of_Ne...	Windows8	History
Mozilla 3 (Windows/Mac)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows8	History
Mozilla 3 (Windows/Mac)	Maya Angelou Program at RIT Canceled - RIT News	http://www.rit.edu/news/story.php?id=49963&so...	Windows8	History
Mozilla 3 (Windows/Mac)	RIT wins National Collegiate Cyber Defense Competition for the first time - RIT News	http://www.rit.edu/news/story.php?id=49964&so...	Windows8	History

Figure 61 Firefox History

As previously mentioned the places.sqlite database files contain information regarding web browsing history; that file also contains information pertaining to a user's Firefox bookmarks. From the EnCase records processor we can see that Facebook, RIT News, Twitter, and Wikipedia are among the Firefox bookmarks on the Windows 8 virtual machine:

Browser Type	Created	Title	Url Name	Profile Name	Internet Artifact Type
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM	Facebook	https://www.facebook.com/	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM	Gmail: Email from Google	https://accounts.google.com/ServiceLogin?service=mail&passive=true&r...	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM	Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=13665749...	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM	Twitter	https://twitter.com/	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM		http://www.mozilla.com/en-US/firefox/customize/	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM		http://www.mozilla.com/en-US/firefox/community/	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:39PM			Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM		place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folde...	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM		place:type=6&sort=14&maxResults=10	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM			Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:39PM			Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM		http://www.mozilla.com/en-US/firefox/help/	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:39PM			Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM		http://www.mozilla.com/en-US/about/	Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:39PM			Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:39PM			Windows8	Bookmarks
Mozilla 3 (Windows/Mac)	04/21/13 04:13:40PM			Windows8	Bookmarks

Figure 62 Firefox Favorites

Viewing Firefox's web cache or temporary Internet files can be found within C:\Users\Windows

8\AppData\Local\Mozilla\Firefox\Profiles\<random text>.default\Cache. EnCase then examined the files contained within the directory and uncovered cached pages for RIT, Twitter, Google, and several other web sites:

Browser Type	Created	Url Name	Internet Artifact Type	Profile Name
Mozilla (Windows/Mac)	05/03/13 05:03:38PM	anon&uri=https://snippets.mozilla.com/3/Firefox/20.0.1/20130409194949/WINNT_x86-msvc/en-US/rel...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/21/13 04:10:38PM	http://www.mozilla.org/en-US/firefox/20.0.1/firstrun/	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/24/13 09:13:15PM	http://en.wikipedia.org/wiki/Military_history_of_Australia_during_World_War_II	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/03/13 05:29:09PM	https://www.facebook.com/ai.php?aed=AQKY0o66ExF5BAo8wZTX2IgFx4bOcJNAKwi4lzCobx6CcCRCH...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/26/13 11:56:46AM	https://www.facebook.com/ai.php?aed=AQLbntVvThXn1fWGqxujzCfLzoPq86sXDCAP1m6AYWUEeXZ_...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/01/13 11:46:52AM	http://en.wikipedia.org/wiki/If_Day	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/02/13 11:32:27AM	https://www.facebook.com/ai.php?aed=AQLuHVNLHhWf8mM87GnZHojEbo17gh5FmTYKPfqG_nWI3I...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/25/13 10:20:49PM	https://www.facebook.com/ai.php?aed=AQI6Wga2Ujk9Mdkuv9eBxomDaf1n9KcTc_1UeWgrQ3FLyWni...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/02/13 11:25:46AM	http://en.wikipedia.org/wiki/United_States_v._The_Progressive	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/03/13 05:29:23PM	https://www.facebook.com/ai.php?aed=AQJ9m_gtjgHwyXJ53_Xzc8zSLJAtz3Spb3p1aCC6-7bKOTPNfg0...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/21/13 04:52:11PM	http://www.rit.edu/news/story.php?id=49951&source=enewsletter	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:39PM	http://platform.twitter.com/widgets/hub.html	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/24/13 09:40:53PM	https://www.facebook.com/ai.php?aed=AQKYOTZJ7RDarcx2O_ARDJff1-xi_iRpPkjEne4O4qYkWqMH3U...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/03/13 05:24:08PM	http://platform.twitter.com/widgets/tweet_button.1367516458.html	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:40PM	https://platform.twitter.com/widgets/hub.html	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/25/13 10:21:01PM	http://www.rit.edu/news/story.php?id=49671&source=enewsletter	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/24/13 09:40:32PM	http://www.rit.edu/news/story.php?id=49958&source=enewsletter	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/01/13 11:47:32AM	https://www.facebook.com/ai.php?aed=AQLjmEk_zAAsnbIXZjsPfIVrmsMQVXHWL6QyHkzjHNOy-3N86...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:35PM	http://www.rit.edu/imagine/	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:11PM	http://www.rit.edu/news/nandedaily.php	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:11:26PM	http://en.wikipedia.org/wiki/Main_Page	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/23/13 10:33:33PM	http://en.wikipedia.org/wiki/Alcohol_laws_of_New_Jersey	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:24PM	https://www.facebook.com/ai.php?aed=AQK12xu95kDUkd_Rw_klTrH2DsgfsQE4Zy8z2htuiKkqUGJ9oI...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/21/13 04:52:13PM	http://ct1.addthis.com/static/r07/sh114.html	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/21/13 04:52:14PM	http://platform.twitter.com/widgets/tweet_button.1366232305.html	Cache\HTML	Windows8
Mozilla (Windows/Mac)	04/26/13 11:55:37AM	https://www.facebook.com/ai.php?aed=AQJdlhQJXcgcoQjApD_xPNQUiR7fJXc2AbtR52OMPPURFcQ4...	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:34PM	http://www.rit.edu/news/story.php?id=49994&source=enewsletter	Cache\HTML	Windows8
Mozilla (Windows/Mac)	05/04/13 03:52:36PM	http://www.rit.edu/template/v1/images/favicon.ico	Cache\HTML	Windows8

Figure 63 Firefox Cache

When I took a look at the gallery option for Firefox's web cache, I found images from the many websites visited during the data generation process:

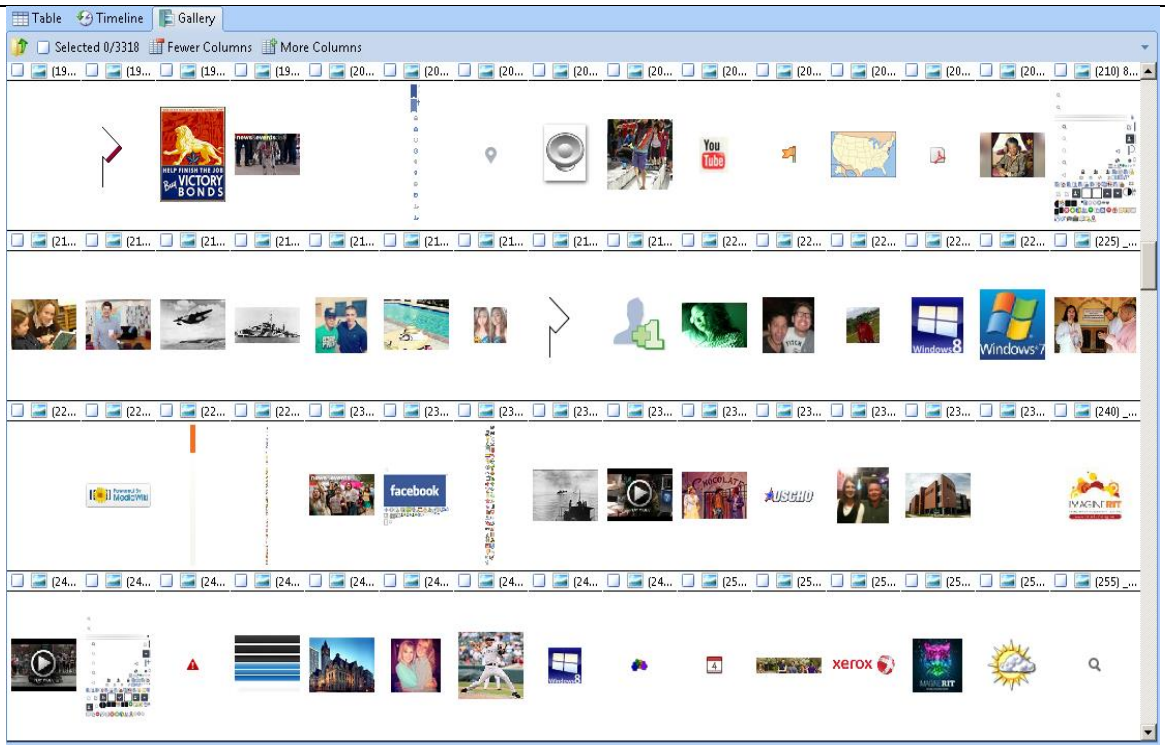


Figure 64 Firefox Cached Images

One of the more interesting artifacts that I was able to find using the EnCase records processor was information regarding Firefox login data. It appears that Firefox stored information regarding Facebook login credentials. This is especially interesting because I instructed Firefox to remember usernames and passwords for both Facebook and Twitter; yet EnCase only found the stored Facebook credentials. It should be noted that these credentials are not stored in plaintext. The values of the username and password are encrypted:

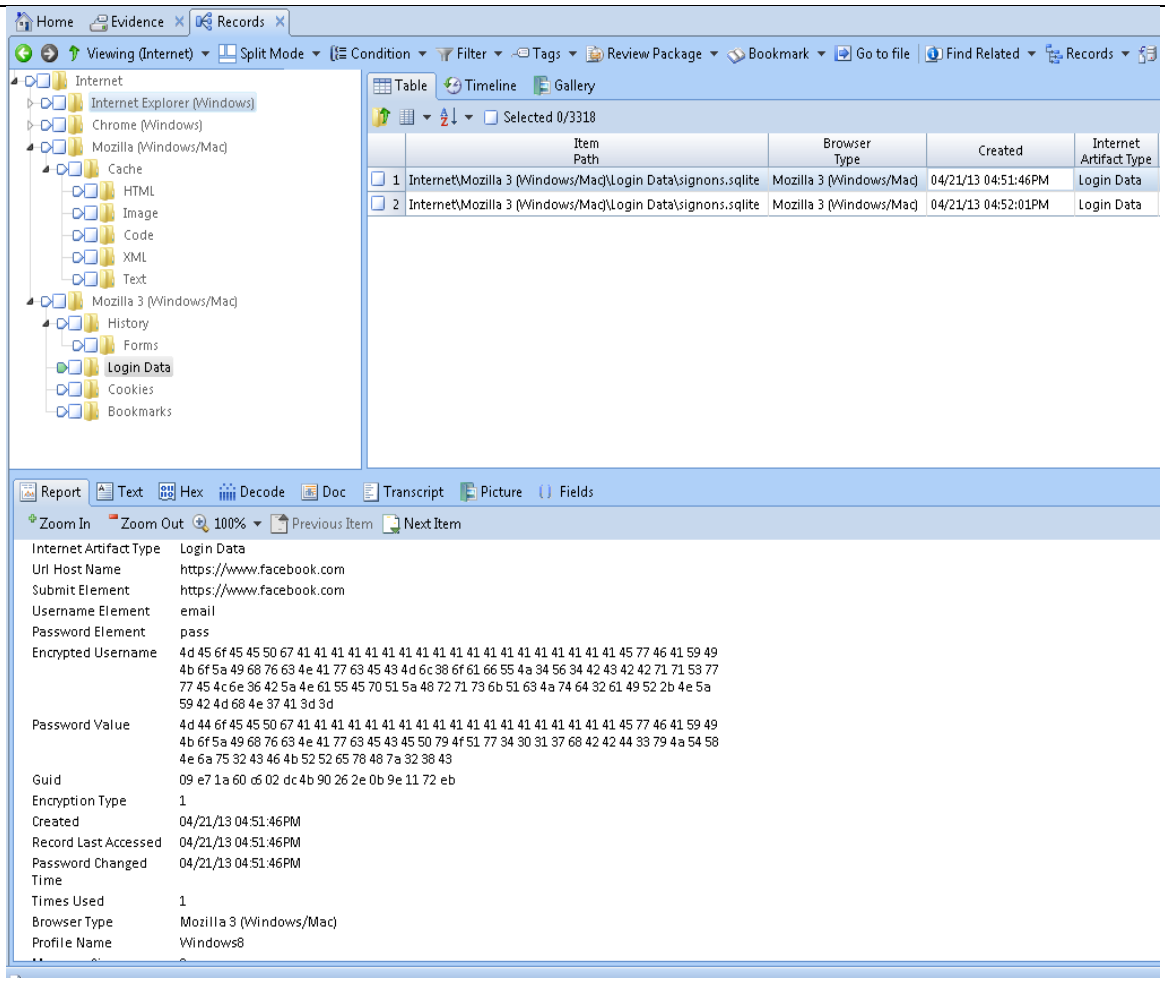


Figure 65 Firefox Stored Login Data

Chrome

Like Firefox, the Chrome web browser stores information within the user's profile. In the case of the Wndows 8 virtual machine, that location is C:\Users\AppData\Windows 8\Local\Google\Chrome\User Data. From this directory, we are able to find history, favorites, and cache of Chrome. Using the EnCase records processor I was able to recover a complete browsing history for Chrome with accessed date/time. We are able to see that during the data generation process Chrome was used to visit Twitter, RIT News, Facebook, Wikipedia, and several other websites:

Browser Type	Title	Accessed	Url Name	Internet Artifact Type
Chrome (Windows)	Twitter	05/04/13 03:54:09PM	https://twitter.com/	History
Chrome (Windows)	Untying the secret of Celtic knots - RIT News	05/04/13 03:53:23PM	http://www.rit.edu/news/story.php?id=49994&source=enewsle...	History
Chrome (Windows)	RIT - Imagine RIT: Innovation and Creativity Festival	05/04/13 03:53:21PM	http://www.rit.edu/imagine/	History
Chrome (Windows)	Facebook	05/04/13 03:53:20PM	https://www.facebook.com/	History
Chrome (Windows)	Twitter	05/04/13 03:53:14PM	https://twitter.com/	History
Chrome (Windows)	Facebook	05/04/13 03:53:08PM	https://www.facebook.com/	History
Chrome (Windows)	RIT News - News & Events Daily	05/04/13 03:53:08PM	http://www.rit.edu/news/nandedaily.php	History
Chrome (Windows)	George Harrison - Wikipedia, the free encyclopedia	05/04/13 03:53:08PM	http://en.wikipedia.org/wiki/George_Harrison	History
Chrome (Windows)	Wikipedia, the free encyclopedia	05/04/13 03:53:03PM	http://en.wikipedia.org/wiki/Main_Page	History
Chrome (Windows)	Twitter	05/03/13 05:27:38PM	https://twitter.com/	History
Chrome (Windows)	Eight Beat Measure celebrates 25 years - RIT News	05/03/13 05:24:49PM	http://www.rit.edu/news/story.php?id=49993&source=enewsle...	History
Chrome (Windows)	RIT's 2013 Innovation Hall of Fame induction is Friday - RIT News	05/03/13 05:24:49PM	http://www.rit.edu/news/story.php?id=49992&source=enewsle...	History
Chrome (Windows)	Keith Motley, University of Massachusetts chancellor, keynotes RIT's 20...	05/03/13 05:24:43PM	http://www.rit.edu/news/story.php?id=49957&source=enewsle...	History
Chrome (Windows)	Facebook	05/03/13 05:24:17PM	https://www.facebook.com/	History
Chrome (Windows)	Mother India - Wikipedia, the free encyclopedia	05/03/13 05:24:07PM	http://en.wikipedia.org/wiki/Mother_India	History
Chrome (Windows)	Twitter	05/03/13 05:23:51PM	https://twitter.com/	History
Chrome (Windows)	RIT News - News & Events Daily	05/03/13 05:23:49PM	http://www.rit.edu/news/nandedaily.php	History
Chrome (Windows)	Wikipedia, the free encyclopedia	05/03/13 05:23:49PM	http://en.wikipedia.org/wiki/Main_Page	History
Chrome (Windows)	Facebook	05/03/13 05:23:49PM	https://www.facebook.com/	History
Chrome (Windows)	Twitter	05/02/13 11:35:35AM	https://twitter.com/	History
Chrome (Windows)	(1) WindowsEight Forensics	05/02/13 11:35:09AM	https://www.facebook.com/windowseight.forensics	History
Chrome (Windows)	(1) WindowsEight Forensics	05/02/13 11:35:07AM	https://www.facebook.com/windowseight.forensics	History
Chrome (Windows)	Facebook	05/02/13 11:35:06AM	https://www.facebook.com/#/windowseight.forensics	History
Chrome (Windows)	(1) Facebook	05/02/13 11:35:01AM	https://www.facebook.com/?sk=h_chr	History
Chrome (Windows)	Facebook	05/02/13 11:34:57AM	https://www.facebook.com/	History
Chrome (Windows)	(1) Facebook	05/02/13 11:34:41AM	https://www.facebook.com/photo.php?fbid=1015135291619193...	History
Chrome (Windows)	Performing LIVE at RIT: 'Bands on the bricks' - RIT News	05/02/13 11:34:19AM	http://www.rit.edu/news/story.php?id=49984&source=enewsle...	History
Chrome (Windows)	Invisible captioning is the Next Big Idea - RIT News	05/02/13 11:34:10AM	http://www.rit.edu/news/story.php?id=49981&source=enewsle...	History

Figure 66 Chrome History

EnCase easily uncovered the Windows 8 user's Top Sites, which include that user's favorites/bookmarks. In the case of the Window s7 virtual machine we see that Chrome frequently visited Wikipedia, the RIT Mirrors, RIT News, Twitter, and Facebook:

Browser Type	Title	Url Name	Internet Artifact Type
Chrome (Windows)	Wikipedia, the free encyclopedia	http://en.wikipedia.org/wiki/Main_Page	Top Sites
Chrome (Windows)	Index of /	http://mirrors.rit.edu/	Top Sites
Chrome (Windows)	Welcome to Google Chrome	http://www.google.com/chrome/intl/en/welcome.html	Top Sites
Chrome (Windows)	RIT News - News & Events Daily	http://www.rit.edu/news/nandedaily.php	Top Sites
Chrome (Windows)	Performing LIVE at RIT: 'Bands on the bricks' - RIT News	http://www.rit.edu/news/story.php?id=49984&source=enewsle...	Top Sites
Chrome (Windows)	Chrome Web Store	https://chrome.google.com/webstore?hl=en	Top Sites
Chrome (Windows)	Sign In	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1...	Top Sites
Chrome (Windows)	Twitter	https://twitter.com/	Top Sites
Chrome (Windows)	(1) Facebook	https://www.facebook.com/	Top Sites

Figure 67 Chrome Top Sites

From the Chrome User Data directory along with EnCase, it was simple to uncover a listing of web pages that were visited by the user through the use of Chrome's web cache. From this we can see that during the data generation process I visited Wikipedia, Facebook, Twitter, RIT, and many other websites:

Browser Type	Created	Url Name	Internet Artifact Type
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/	Cache\HTML
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/images/sponsors2011/timewarner.gif	Cache\Image
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/images/nav-right.gif	Cache\Image
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/images/nav-left.gif	Cache\Image
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/_site.css	Cache\Code
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/images/2012-header.gif	Cache\Image
Chrome (Windows)	05/04/13 03:54:09PM	https://www.facebook.com/ai.php?aed=AQIIX2RmQsWRPaIH5-lVb_yjCXDohBngloWDL99fLPK...	Cache\HTML
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/images/countdown_bubble.png	Cache\Image
Chrome (Windows)	05/04/13 03:54:09PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/yP/r/HWjpUkpaocI.js	Cache\Code
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/imagine/images/imagine_background_tile.gif	Cache\Image
Chrome (Windows)	05/04/13 03:54:09PM	http://www.rit.edu/news/story.php?id=49994&source=enewsletter	Cache\HTML
Chrome (Windows)	05/04/13 03:54:09PM	https://fbcdn-creative-a.akamaihd.net/hads-ak-prn1/s110x80/735313_6005860724352_624877...	Cache\Image
Chrome (Windows)	05/04/13 03:54:08PM	https://platform.twitter.com/widgets.js	Cache\Code
Chrome (Windows)	05/04/13 03:54:08PM	https://twitter.com/trends?k=3884291836a275e06052793fb472a4&pc=true&src=module	Cache\Code
Chrome (Windows)	05/04/13 03:54:08PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/yr/r/W3Xtq1-pTZj.png	Cache\Image
Chrome (Windows)	05/04/13 03:54:08PM	https://profile-b.xx.fbcdn.net/hprofile-ash3/s32x32/161918_191466437534562_11115_q.jpg	Cache\Image
Chrome (Windows)	05/04/13 03:54:07PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/yR/r/_s4k91A9p_x.js	Cache\Code
Chrome (Windows)	05/04/13 03:54:06PM	https://fbcdn-sphotos-h-a.akamaihd.net/hphotos-ak-ash3/s480x480/524816_10151356643346...	Cache\Image
Chrome (Windows)	05/04/13 03:54:06PM	https://fbcdn-sphotos-f-a.akamaihd.net/hphotos-ak-ash3/s480x480/941764_52155363790196...	Cache\Image
Chrome (Windows)	05/04/13 03:54:05PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/y5/r/ZpsGiyaEt12.png	Cache\Image
Chrome (Windows)	05/04/13 03:54:05PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/yY/r/feV2_mtw08A.js	Cache\Code
Chrome (Windows)	05/04/13 03:54:03PM	https://si0.twimg.com/profile_images/1116013242/Cometa_Michelle_3_normal.jpg	Cache\Image
Chrome (Windows)	05/04/13 03:54:03PM	https://si0.twimg.com/profile_images/2957899179/73ea5ec9789f84955bda576c990763a7_norm...	Cache\Image
Chrome (Windows)	05/04/13 03:54:03PM	https://si0.twimg.com/profile_images/2932402949/8634d1dba79e63c7775646437d012e4f_nor...	Cache\Image
Chrome (Windows)	05/04/13 03:54:03PM	https://si0.twimg.com/profile_images/3506677569/370c15772423bbf33250222ee54d3a14_nor...	Cache\Image
Chrome (Windows)	05/04/13 03:54:03PM	https://si0.twimg.com/profile_images/2350422206/h33iwum9b69ipcvdorfx_normal.jpeg	Cache\Image
Chrome (Windows)	05/04/13 03:54:01PM	http://bits.wikimedia.org/static-1.22wmf2/extensions/TimedMediaHandler/MwEmbedModule...	Cache\Image
Chrome (Windows)	05/04/13 03:54:01PM	http://bits.wikimedia.org/static-1.22wmf2/skins/common/images/icons/fileicon-ogg.png	Cache\Image

Figure 68 Chrome Cache

When I took a look at the gallery option for Chrome's web cache, I found images from the many websites visited during the data generation process:

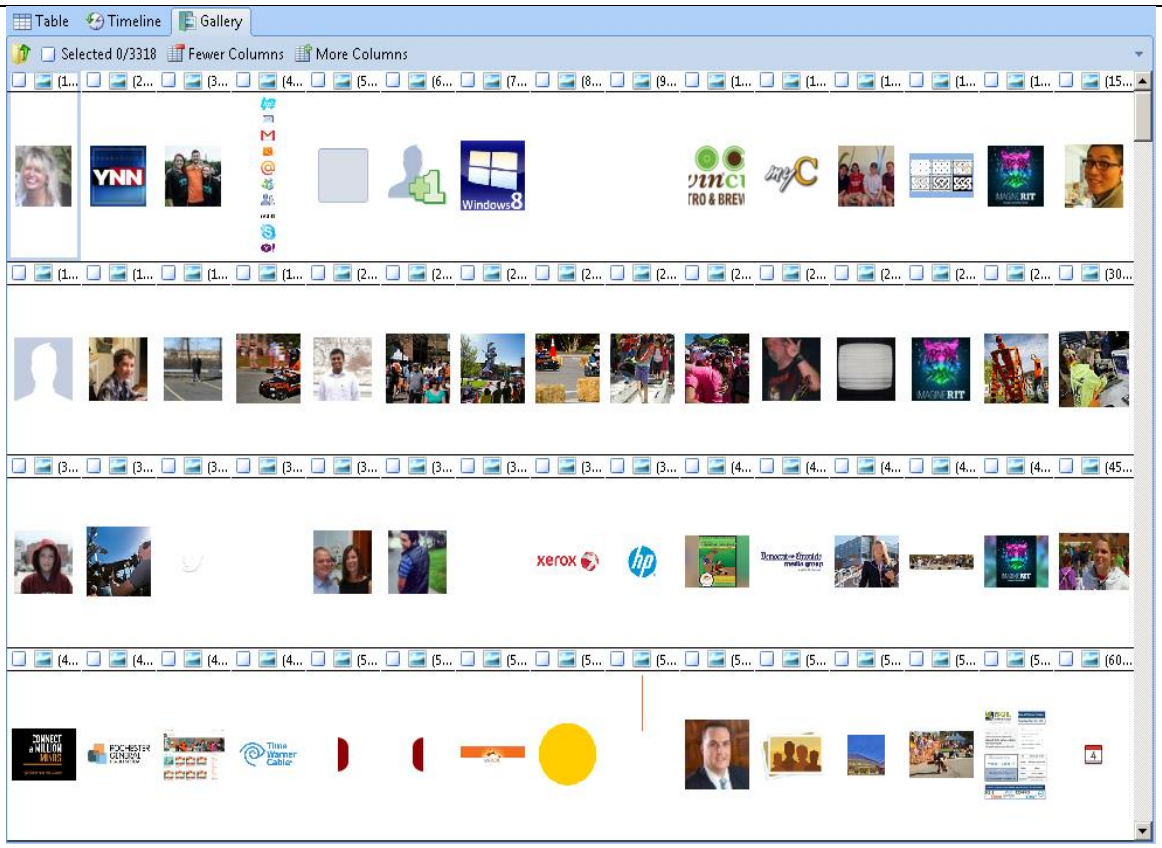


Figure 69 Chrome Cached Images

As was the case with Firefox, Chrome also contained interesting artifacts regarding Chrome login data. It appears that Chrome stored information regarding Facebook and Twitter login credentials. This makes more sense than what I saw with Firefox as I instructed Chrome to remember usernames and passwords for both Facebook and Twitter. As was the case with Firefox and Facebook, the username and password credentials are not stored in plaintext. The values of the username and password are encrypted. What is interesting is the fact that with Twitter the user is stored in plaintext but the password value is encrypted:

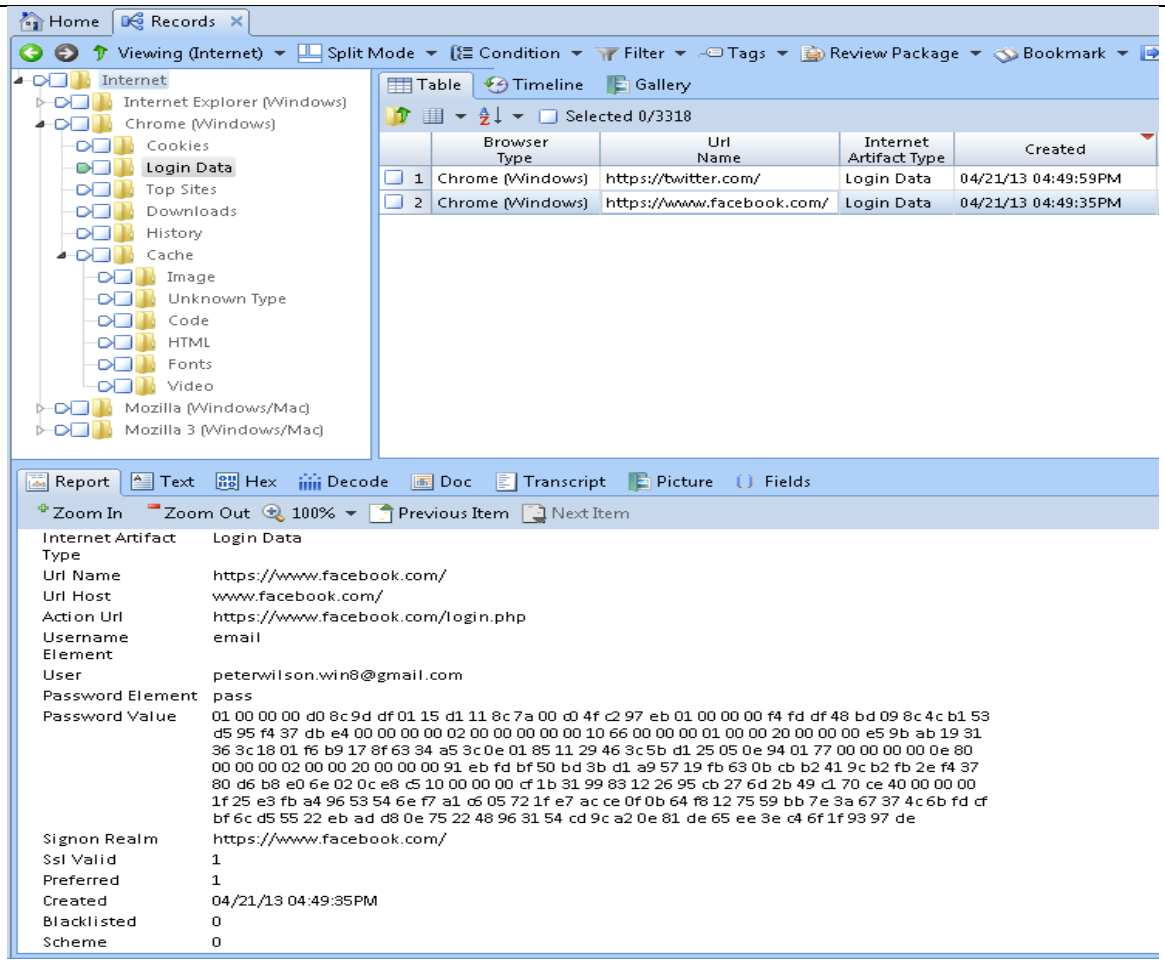


Figure 70 Chrome Login Data

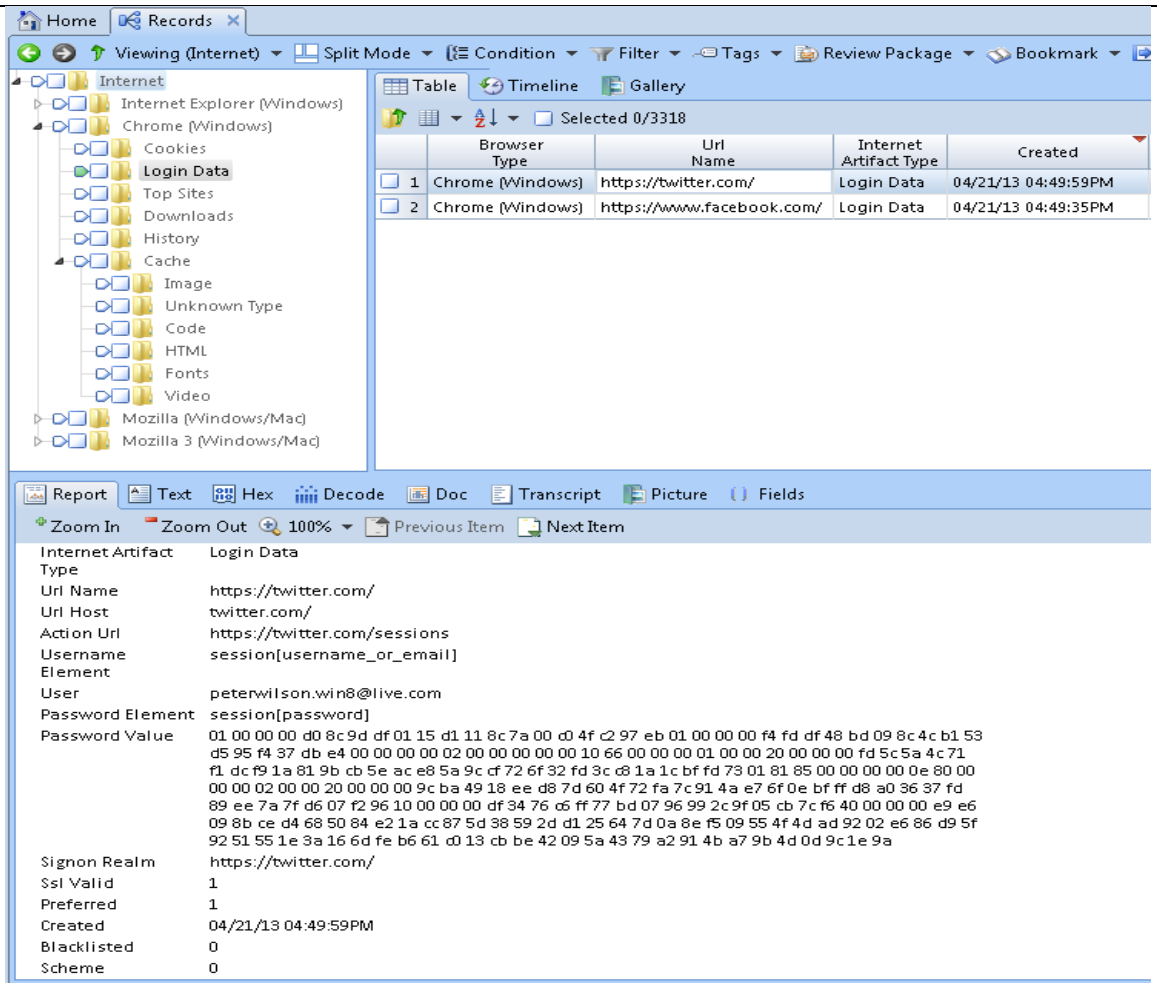


Figure 71 Chrome Login Data

Social Media Items

Finding evidence of social media with FTK wasn't especially difficult. With FTK, I used the Live Search feature along with the keywords "facebook" and "twitter". This enabled be to find artifacts pertaining to those two social media websites. The live search found a total of 10820 hits for the, case insensitive, ANSI, keyword "facebook" within 1137 files and 13049 hits for the, case insensitive, ANSI, keyword "twitter" within 761 files:

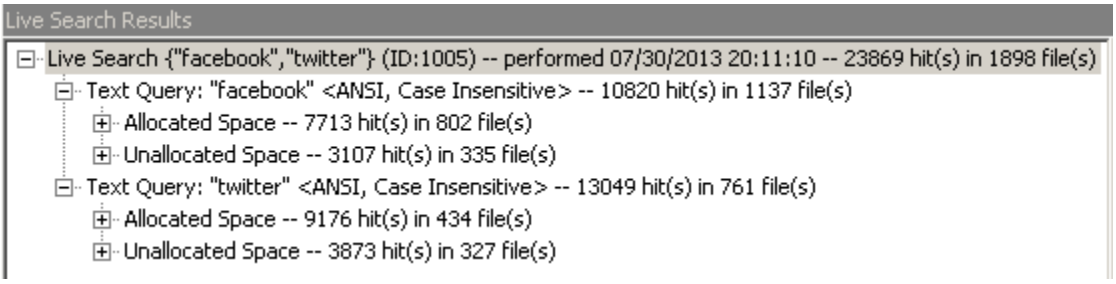


Figure 72 Social Media Items

The majority of the files that I found that contained mention of either Facebook or Twitter were primarily the result of browsing to websites that contained options to share the contents via Facebook or Twitter. There were numerous files with htm, js, css, tmp, and other file extensions but I was unable to uncover any of the specific social

media actions that I took during the data generation process.

While I found quite a bit of evidence that the social media sites of Facebook and Twitter were used, I was unable to uncover any actual Facebook posts, shares, comments, or likes or Twitter tweets, retweets, replies, or favorites. I believe this is the case because the only way through which I accessed the social media sites was through web browsers. While I made updates to social media throughout the course of the data generation process, I suspect very little was actually stored on the hard drive of the Windows 8 virtual machine.

Internet Evidence Finder

Because FTK and EnCase were unable to easily locate evidence pertaining to Internet activity including social media usage, I opted to use Magnet Forensics' Internet Evidence Finder (IEF). This tool was extremely useful in uncover data related to social media activities, finding numerous items for many different, important, categories:

Internet Evidence Finder v6.1
Copyright 2009-2013 Magnet Forensics® Inc.
Build 6.1.1.0033
Case Information Generated At: 08/21/2013 11:39:35
Operating System: Microsoft Windows NT 6.1.7601 Service Pack 1

Selected source:

Windows 8.vmdk - Partition 1 (Microsoft NTFS, 40 GB)

Searches selected:
---
pagefile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:

Windows 8.vmdk - Unpartitioned Space

Searches selected:

Unpartitioned Space

Search items selected:

Browser Activity

Chrome

Facebook Chat

Facebook Email

Facebook Email 'Snippets'

Facebook Pictures

Facebook Status Updates / Wall Posts / Comments

Facebook Web Page Fragments

Firefox

Flash Video Fragments

Gmail

Google Maps

Google Plus

Google Talk

GoogleDocs

GoogleDrive

Hotmail

Internet Explorer 10 History

Internet Explorer v5-9

Internet Explorer v7-v10 InPrivate/Recovery URLs

Pictures

RebuildWeb

SkyDrive

Twitter

Videos

Webpage Recovery

Windows Live Messenger

Output folder: E:\Windows 8 IEF\IEF - Aug 21 2013 113831\

Start time: Aug 21, 2013 11:39:35

End time: Aug 21, 2013 16:51:09

Duration: 05:11:34

Final results of search:

Pictures: 42050 items

Browser Activity: 2138 items

Cloud Services URLs: 3 items

Internet Explorer 10 Carved Content Records: 1698 items

Social Media URLs: 424 items

Facebook Status Updates/Wall Posts/Comments: 26 items

Internet Explorer Typed URLs: 14 items

Parsed Search Queries: 160 items

Videos: 70 items

Internet Explorer Redirect Records: 3 items

Facebook Pages: 10 items

Internet Explorer Cookie Records: 2 items

Internet Explorer 10 Carved History: 244 items

Facebook URLs: 702 items

Facebook Chat: 1013 items

Internet Explorer 10 History: 688 items

Internet Explorer 10 Content: 5974 items

Internet Explorer 10 Cookies: 91 items

Rebuilt Webpages: 287 items

Internet Explorer Cookies: 92 items

Chrome Bookmarks: 6 items

Chrome Cookies: 71 items

Chrome FavIcons: 54 items

Chrome Web History: 159 items

Chrome History Index: 59 items

Chrome Logins: 2 items

Chrome/360 Safe Browser Carved Web History: 172 items

Chrome Top Sites: 9 items

Chrome Autofill: 2 items

IE InPrivate/Recovery URLs: 254 items

Facebook Pictures: 426 items

Firefox Cookies: 110 items

Firefox FormHistory: 2 items

Firefox Web History: 97 items

Firefox Bookmarks: 17 items

Firefox FavIcons: 10 items

Firefox Downloads: 1 items

Firefox SessionStore Artifacts: 144 items

Chrome Cache Records: 1428 items

Firefox Cache Records: 1340 items

Twitter: 27 items

Figure 73 Windows 8 IEF Case Summary

Facebook Activity

Using IEF, I was able to uncover a total of 11 posts or comments that were made as part of the data generation process. Some of the posts or comments were made by the WindowsSeven Forensics Facebook user, while others were made by the WindowsEight Forensics user. I believe this is the case because these two fictional users were friends with each other on Facebook so they would have seen each other's posts and/or comments. I find it especially interesting that when an actual post is made the Sender Name is known, but the Date/Time when it was posted is not, whereas when a comment is made, the Sender Name is unknown, but the Date/Time is. In the figure below, the 11 posts/comments can be seen.

#	Sender ID	Sender Name	Status Update / Wall Post / Comment	Posted Date/Time - (UTC) (MM/dd/yyyy)	Source	Located At
4	100005359690264	WindowsEight Forensics	05/01/2013 Daily Post From Chrome		Windows 8.vmdk - Partition 1 ...	Physical Sector 43299...
5	100005359690264	WindowsEight Forensics	05/02/2013 Daily post From Firefox		Windows 8.vmdk - Partition 1 ...	Physical Sector 46040...
6	100005370100122	WindowsSeven Forensics	05/02/2013 Daily Post from Firefox		Windows 8.vmdk - Partition 1 ...	Physical Sector 46040...
8	100005359690264	n/a	Comment from Firefox	05/02/2013 03:33:18 PM	Windows 8.vmdk - Partition 1 ...	Physical Sector 46041...
9	100005370100122	n/a	Comment from Firefox	05/02/2013 03:17:13 PM	Windows 8.vmdk - Partition 1 ...	Physical Sector 46041...
10	100005370100122	WindowsSeven Forensics	05/04/2013 Daily Post from Chrome		Windows 8.vmdk - Partition 1 ...	Physical Sector 44273...
11	100005359690264	WindowsEight Forensics	05/03/2013 Daily Post from People App		Windows 8.vmdk - Partition 1 ...	Physical Sector 44273...
12	100005370100122	WindowsSeven Forensics	05/03/2013 Daily Post From Internet Explorer		Windows 8.vmdk - Partition 1 ...	Physical Sector 44273...
18	100005359690264	n/a	Comment from People App	05/03/2013 11:09:50 PM	Windows 8.vmdk - Partition 1 ...	Physical Sector 44273...
19	100005370100122	n/a	Comment From Internet Explorer	05/03/2013 08:47:33 PM	Windows 8.vmdk - Partition 1 ...	Physical Sector 44273...
20	100005370100122	n/a	Comment from Chrome	05/04/2013 07:43:31 PM	Windows 8.vmdk - Partition 1 ...	Physical Sector 44273...
23	100005359690264	WindowsEight Forensics	05/01/2013 Daily Post From Chrome		Windows 8.vmdk - Partition 1 ...	Physical Sector 33139...

Figure 74 Windows 8 Facebook Activity

Twitter Activity

Using IEF, I was able to uncover a total of 19 tweets and retweets that were made or viewed as part of the data generation process. IEF was able to discover 16 total tweets made from @RITsports or @RITNEWS that were made yet only a single tweet from @Win8Forensics, and 2 tweets from @Win7Forensics. The tweets that are seen, are from the Twitter feed of @Win8Forensics that was accessed through twitter.com as part of the data generation process.

#	Name	Screen Name	Created Date/Time - (UTC) (MM/dd/yyyy)	Tweet Text	Source	Located At
1	RIT Sports Info	@RITsports	04/21/2013 09:20:53 PM	BB | <a href="/search?q=%23RIT&src=hash" data-query-so...	Windows 8.vmdk - Partition 1 ...	File offset 8882986
2	RIT Sports Info	@RITsports	04/25/2013 10:47:06 PM	<a href="/search?q=%23RIT&src=hash" data-query-source...	Windows 8.vmdk - Partition 1 ...	File offset 123181593
3	RIT Sports Info	@RITsports	04/25/2013 10:45:31 PM	BB | <a href="/FisherAthletics" class="twitter-atreply pretty-li...	Windows 8.vmdk - Partition 1 ...	File offset 123187185
4	Windows 8 Forensics	@Win8Forensics	05/04/2013 07:53:17 PM	05/04/2013 Daily Tweet from Firefox	Windows 8.vmdk - Partition 1 ...	Physical Sector 26282...
5	RIT NEWS	@RITNEWS	05/04/2013 07:28:27 PM	RT <a href="/DandC" class="twitter-atreply pretty-link" dir=...	Windows 8.vmdk - Partition 1 ...	Physical Sector 26768...
8	RIT Sports Info	@RITsports	05/04/2013 07:17:30 PM	<a href="/search?q=%23RIT&src=hash" data-query-source...	Windows 8.vmdk - Partition 1 ...	Physical Sector 26768...
9	RIT Sports Info	@RITsports	05/04/2013 07:11:51 PM	<a href="/search?q=%23RIT&src=hash" data-query-source...	Windows 8.vmdk - Partition 1 ...	Physical Sector 26768...
10	Windows 7 Forensics	@Win7Forensics	05/04/2013 07:44:05 PM	05/04/2013 Daily Tweet from Firefox	Windows 8.vmdk - Partition 1 ...	Physical Sector 26814...
11	RIT Sports Info	@RITsports	05/04/2013 07:42:14 PM	U of R scores in the bottom of the 5th to tie the game again...	Windows 8.vmdk - Partition 1 ...	Physical Sector 26814...
12	RIT Sports Info	@RITsports	05/04/2013 06:57:06 PM	<a href="/search?q=%23LLWTennisChampionship&src=ha...	Windows 8.vmdk - Partition 1 ...	Physical Sector 29306...
13	RIT Sports Info	@RITsports	05/04/2013 06:54:48 PM	<a href="/search?q=%23LLWTennisChampionship&src=ha...	Windows 8.vmdk - Partition 1 ...	Physical Sector 29307...
16	RIT Sports Info	@RITsports	05/04/2013 05:52:21 PM	<a href="/search?q=%23LLWTennisChampionship&src=ha...	Windows 8.vmdk - Partition 1 ...	Physical Sector 29307...
18	RIT NEWS	@RITNEWS	05/04/2013 05:19:39 PM	Coverage of <a href="/Imagine_RIT" class="twitter-atreply ...	Windows 8.vmdk - Partition 1 ...	Physical Sector 29307...
20	RIT Sports Info	@RITsports	05/04/2013 04:34:42 PM	BB | <a href="/search?q=%23RIT&src=hash" data-query-so...	Windows 8.vmdk - Partition 1 ...	Physical Sector 29307...
23	RIT Sports Info	@RITsports	05/03/2013 08:56:08 PM	At halftime, <a href="/RITMensLax" class="twitter-atreply p...	Windows 8.vmdk - Partition 1 ...	Physical Sector 43298...
24	RIT Sports Info	@RITsports	05/04/2013 04:21:47 PM	<a href="/search?q=%23LLWTennisChampionship&src=ha...	Windows 8.vmdk - Partition 1 ...	Physical Sector 34375...
25	Windows 7 Forensics	@Win7Forensics	05/01/2013 03:28:57 PM	<a href="/Win7Forensics" class="twitter-atreply pretty-link" ...	Windows 8.vmdk - Partition 1 ...	Physical Sector 22051...
26	RIT Sports Info	@RITsports	04/21/2013 09:20:53 PM	BB | <a href="/search?q=%23RIT&src=hash" data-query-so...	Windows 8.vmdk - Partition 1 ...	Physical Sector 97890...
27	RIT Sports Info	@RITsports	05/03/2013 08:56:08 PM	At halftime, <a href="/RITMensLax" class="twitter-atreply p...	Windows 8.vmdk - Partition 1 ...	Physical Sector 25220...

Figure 75 Windows 8 Twitter Activity

Facebook URLs

While using IEF, I was able to uncover 1189 specific Facebook URLs from Carved History or ecorded Browser Activity including the following potential activities:

- At Facebook home page
- Failed to log onto Facebook

- Looking at Facebook group…
- Looking at Facebook maps…
- Looking at Facebook photo…
- Looking at Facebook profile…
- Typing in search values:
- Unknown

These 8 different types of potential activities are categories that IEF uses to classify the data that it has carved from Internet Explorer, Firefox, or Chrome browser activities and/or history. In the figure below, I've selected at least one of each category to show what information IEF was able to discover:

#	URL	Potential Activity	Artifact	Artifact ID	Date/Time - (UTC) (MM/dd/yyyy)	Source
52	https://www.facebook.com/?sk=welcome	At Facebook home page	Internet Explorer 10 History	188		Windows 8.vmdk ...
345	https://www.facebook.com/	At Facebook home page	Chrome Web History	39	04/21/2013 08:46:57 PM	Windows 8.vmdk ...
402	https://www.facebook.com/	At Facebook home page	Firefox Web History	32	04/24/2013 02:34:37 AM	Windows 8.vmdk ...
113	https://www.facebook.com/login.php?login_attempt=1	Failed to log onto Facebook	Internet Explorer 10 History	344		Windows 8.vmdk ...
347	https://www.facebook.com/login.php?login_attempt=1	Failed to log onto Facebook	Chrome Web History	46	04/21/2013 08:49:24 PM	Windows 8.vmdk ...
47	http://www.facebook.com/groups/288032781277841/454...	Looking at Facebook group with group id: 288032781277841	Internet Explorer 10 History	128		Windows 8.vmdk ...
182	https://www.facebook.com/places/map_iframe.php?locale...	Looking at Facebook maps of profile id: places	Internet Explorer 10 History	498		Windows 8.vmdk ...
54	https://www.facebook.com/photo.php?fbid=10151345109...	Looking at Facebook photo with id: 10151345109771930, album id...	Internet Explorer 10 History	190		Windows 8.vmdk ...
49	https://www.facebook.com/ISTatRIT	Looking at Facebook profile with profile id: ISTatRIT	Internet Explorer 10 History	185		Windows 8.vmdk ...
351	https://www.facebook.com/windowseight.forensics	Looking at Facebook profile with profile id: windowseight.forensics	Chrome Web History	53	04/21/2013 08:50:54 PM	Windows 8.vmdk ...
415	https://www.facebook.com/windowseight.forensics	Looking at Facebook profile with profile id: windowseight.forensics	Firefox Web History	90	05/03/2013 09:28:18 PM	Windows 8.vmdk ...
608	https://www.facebook.com/ajax/typeahead/search.php?v...	Typing in search values: Commen	Browser Activity	1997		Windows 8.vmdk ...
471	https://www.facebook.com/ajax/typeahead/search.php?v...	Typing in search values: Daily	Browser Activity	1746		Windows 8.vmdk ...
474	https://www.facebook.com/ajax/typeahead/search.php?v...	Typing in search values: Post	Browser Activity	1749		Windows 8.vmdk ...
444	http://www.facebook.com/plugins/like.php?href=http%3A%...	Unknown	Browser Activity	1196		Windows 8.vmdk ...

Figure 76 Windows 8 Facebook URLs

In some cases, the URLs are still active and can be used to view what the user was looking at. In addition, we are also able to see some of the keyboard activity of the user in the form of the "Typing in search values:" Potential Activity. This would be especially useful to an investigator.

IEF Timeline

One of the really great features of IEF is its ability to create a timeline of activity for the artifacts that it's uncovered. Using the IEF Timeline application, an investigator can review the activities that took place on a given day, at a given time, and pertaining to specific aspects of Internet acitivity. For example, in the figure below, I've elected to see a timeline of Facebook URLs, Facebook Status Updates/Wall Posts/Comments, and Twitter from April 20th, 2013 to May 6th, 2013 (the time period in which the data generation process took place).

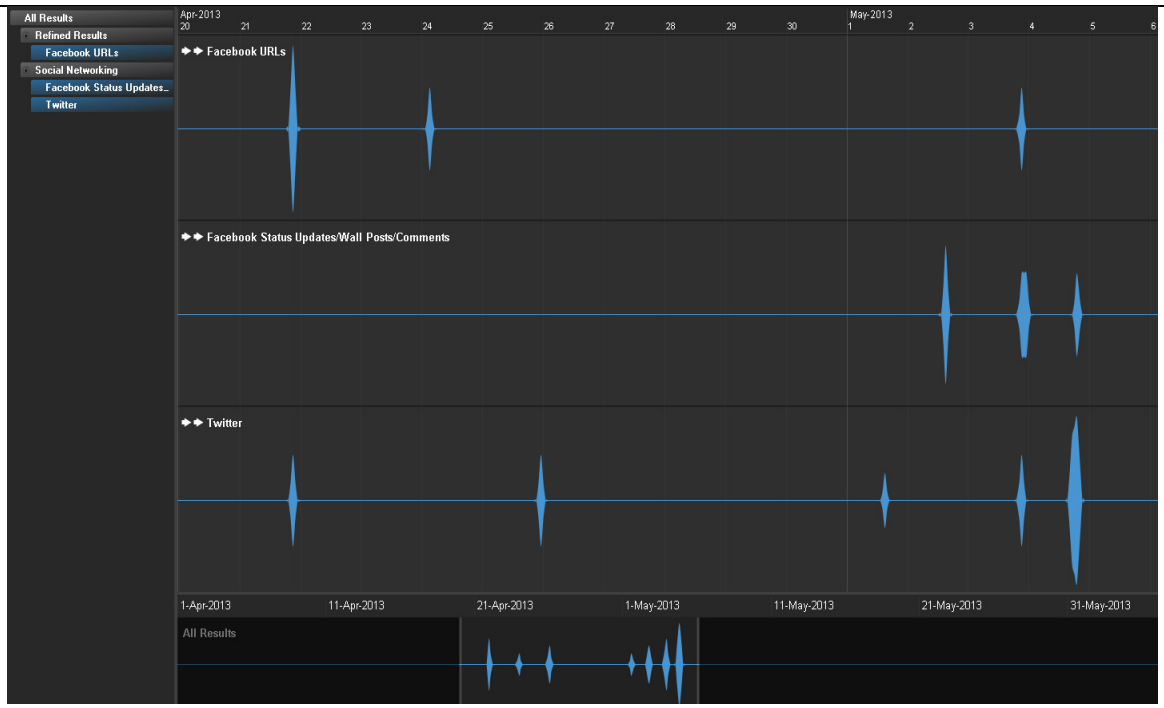


Figure 77 IEF Timeline for Social Media

From this timeline, I can then drill down into specific records for each of the different categories to find out what activities took place on a given day at a given time:

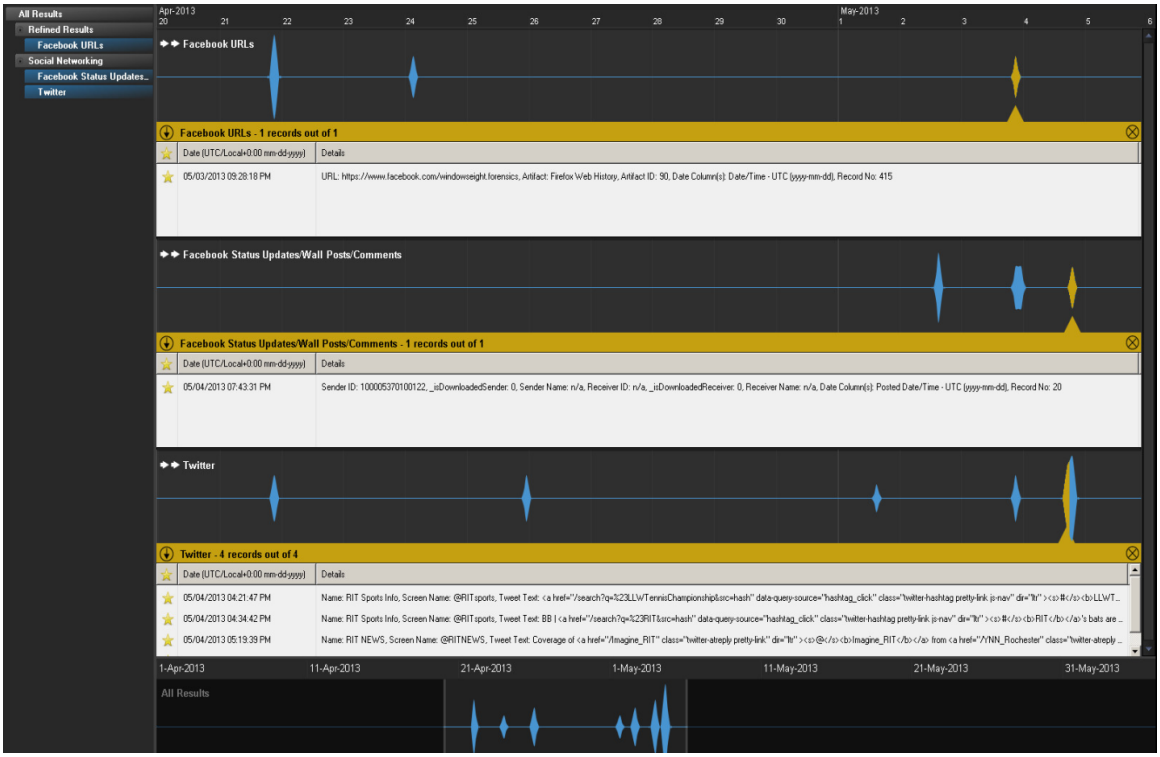


Figure 78 IEF Timeline for Social Media Items with Details

Email

Another set of artifacts that I worked on recovering were email artifacts. During the data generation process I sent and received many emails from both the Windows 8 Gmail and Live email accounts using the Mail App. Using FTK, and its ability to locate email items, I was able to recover the emails that I sent and received. FTK divided the emails based upon recipient email addresses, so I was able to view email that was received by the Windows 8 Gmail and Live accounts as well as email that was sent to the Windows 7 Gmail and Live accounts from the Windows 8 email accounts.

In the case of email sent to peterwilson.win8@gmail.com, FTK found a total of 46 emails. Most of these emails were from the accounts that I created for the purpose of data generation but a few others were from Facebook, Twitter, or the email provider:

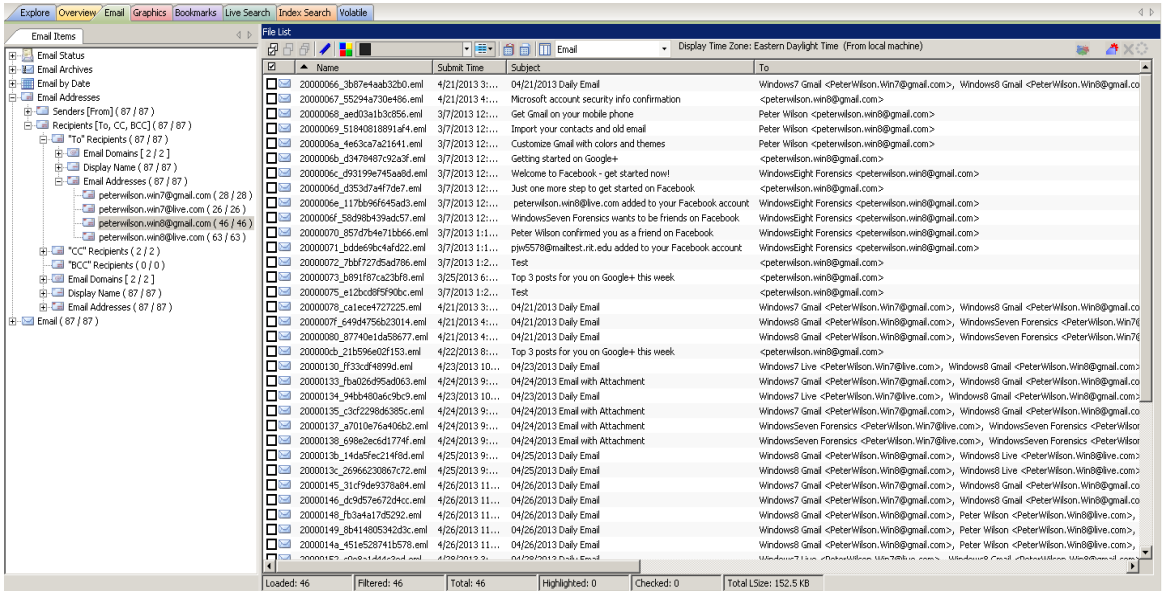


Figure 79 Email sent to peterwilson.win8@gmail.com

In the case of email sent to peterwilson.win8@live.com, FTK found a total of 63 emails. Most of these emails were from the accounts that I created for the purpose of data generation but a few others were from Facebook, Twitter, or the email provider:

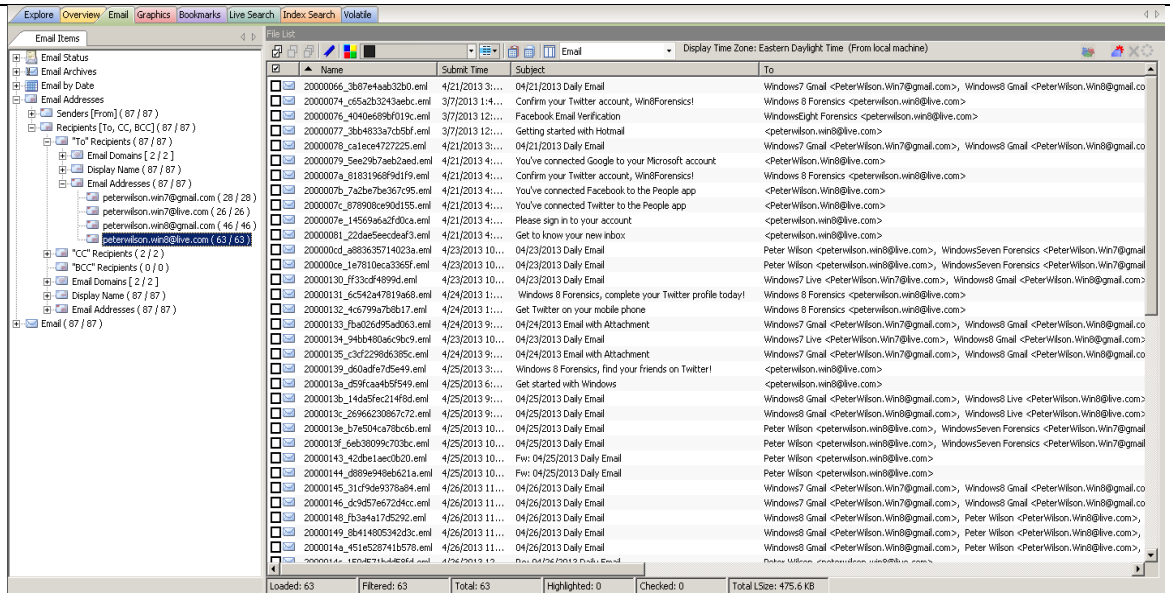


Figure 80 Email sent to peterwilson.win8@live.com

In the case of email sent from peterwilson.win8@gmail.com, FTK found a total of 23 emails. All of the emails sent from this accounts were sent to accounts that I created for the purpose of data generation:

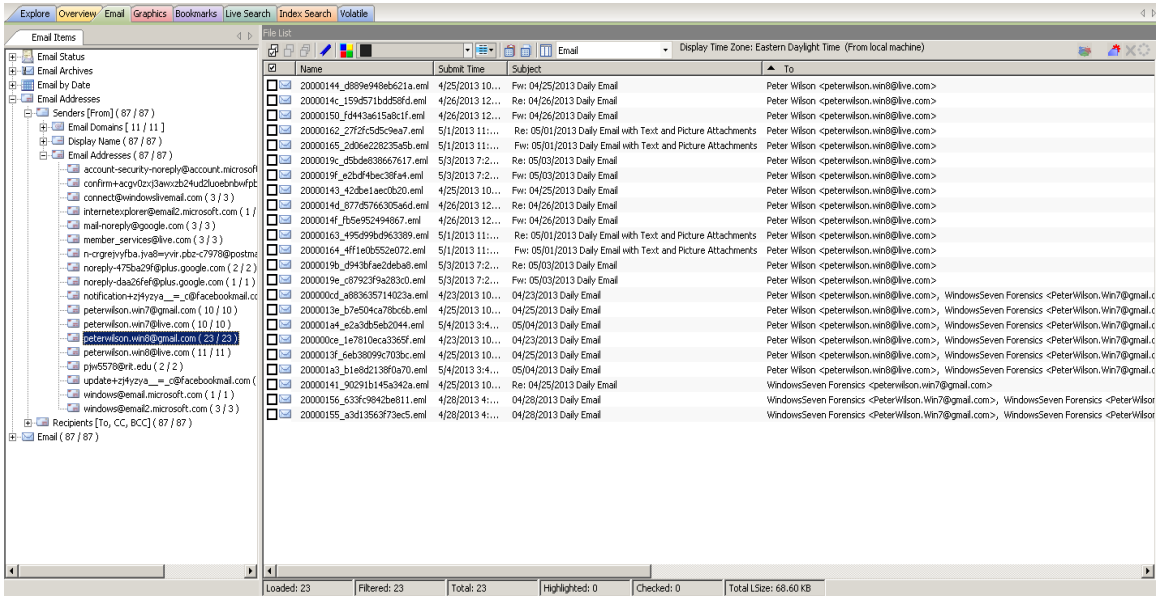


Figure 81 Email sent from peterwilson.win8@gmail.com

In the case of email sent from peterwilson.win8@;live.com, FTK found a total of 11 emails. All of the emails sent from this accounts were sent to accounts that I created for the purpose of data generation:

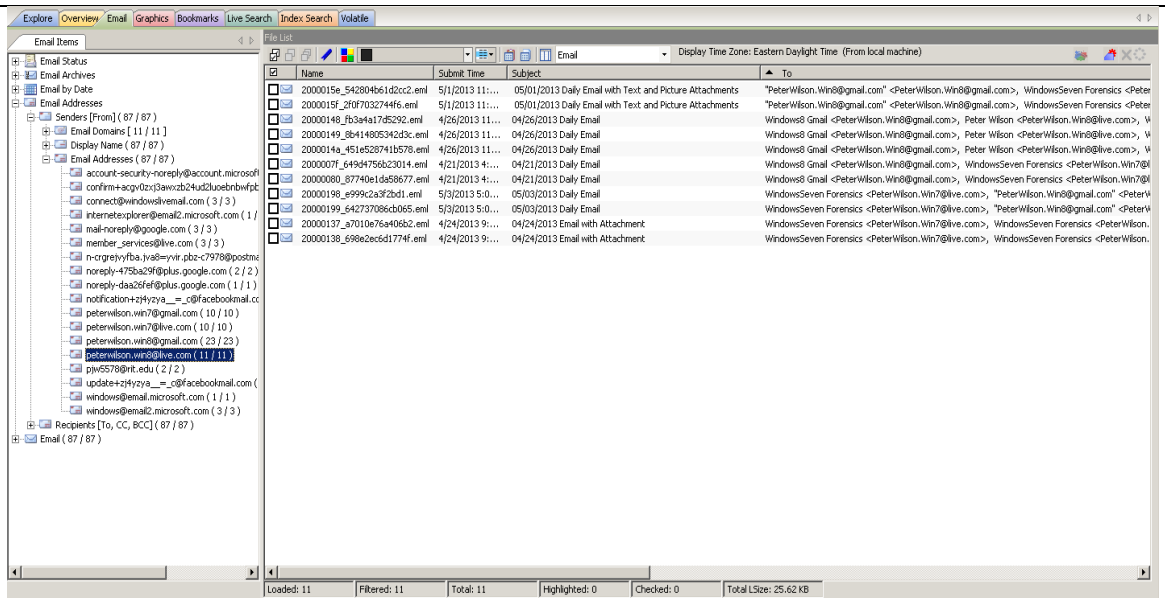


Figure 82 Email sent from peterwilson.win8@live.com

FTK found a total of 8 emails that were forwards of previously sent emails. In all of the emails, the receiver was peterwilson.win8@live.com:

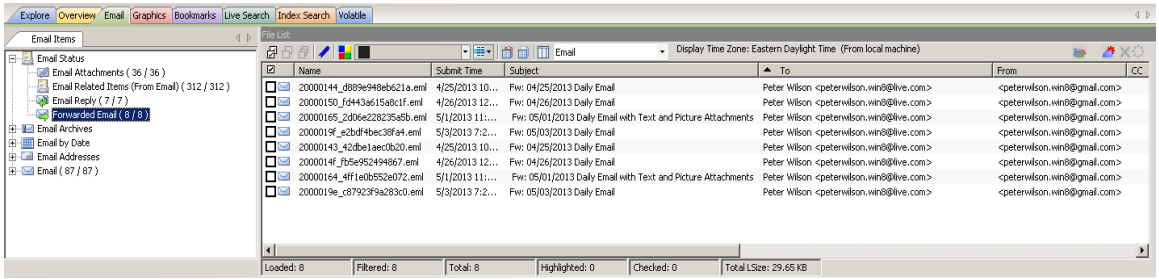


Figure 83 Forwarded Emails

FTK found a total of 7 emails that were replies to previously sent emails. In all of the emails, the receiver was either peterwilson.win7@gmail.com or peterwilson.win8@live.com:

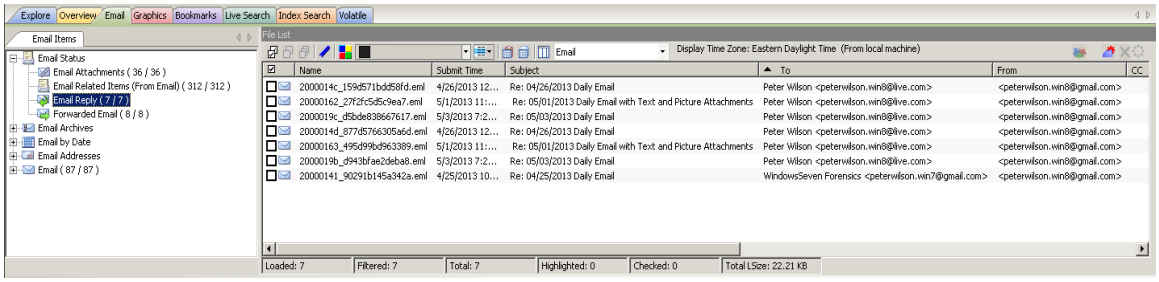


Figure 84 Replied Emails

In the case of Windows 8, FTK recovered a total of 36 email attachments:

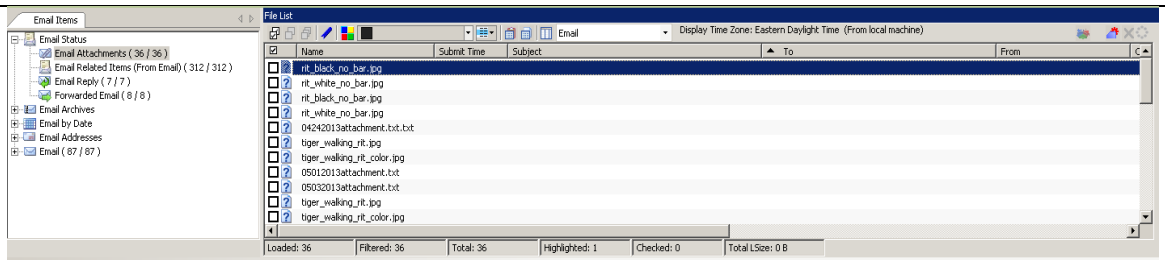


Figure 85 Email Attachments

Unfortunately, when I view an email that would have had an attachment sent with it I see information pertaining to the attachment, but am unable to view the attachments themselves:

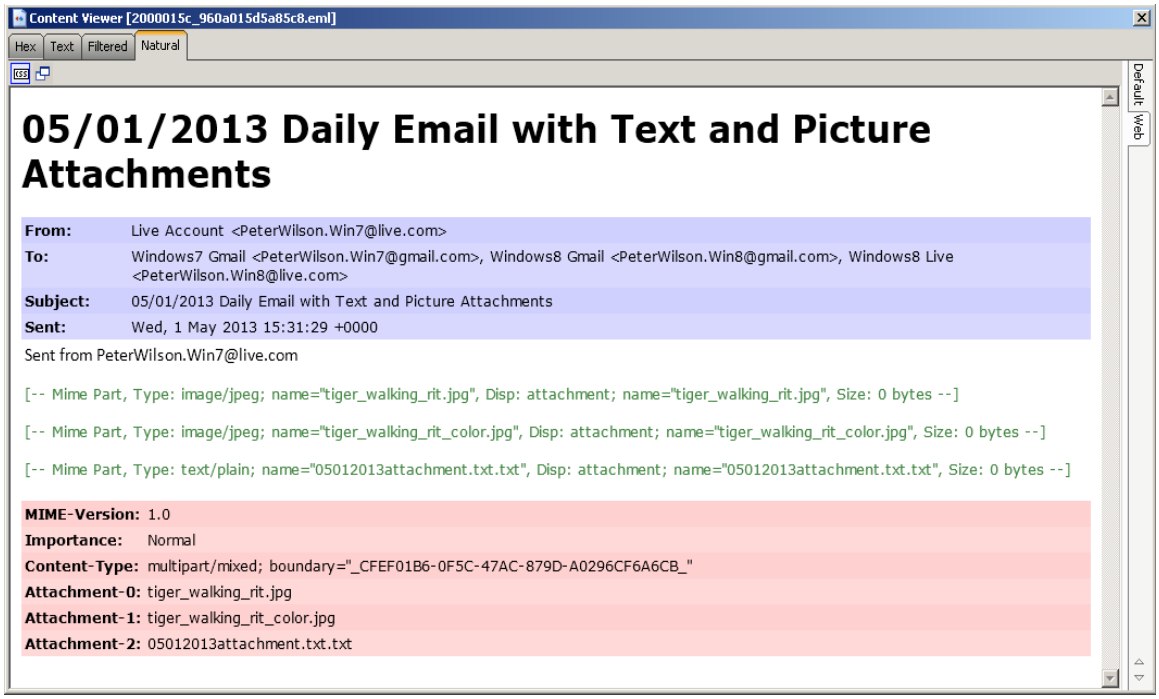


Figure 86 Recovered Email with Attachments

While I was unable to view the actual attachments with the emails that they were attached to, I was able to locate each of the files by doing a keyword search using both EnCase and FTK.

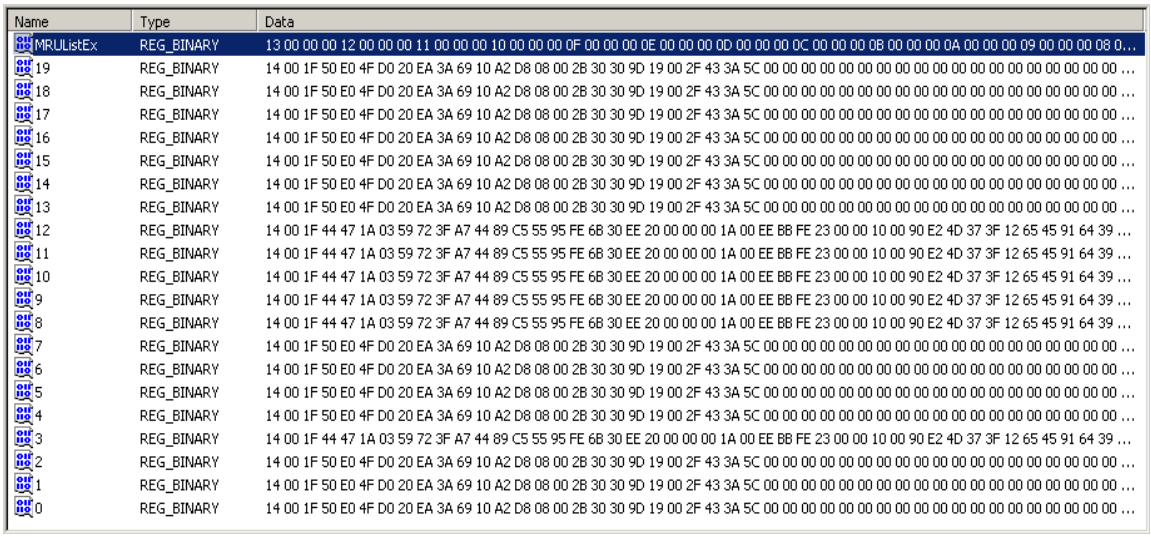
Registry

The Windows registry often contains a lot of information regarding a user's activity on a system. Using the AccessData Regsistry Viewer, along with an exported versions of the Windows 8 registry hives I was able to uncover several pieces of information that would be useful to a forensic investigator.

Windows 8 User Hive

The Windows 8 User hive (NTUSER.dat) found within the C:\Users\Windows7 directory as NTUSER.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 8 virtual machine.

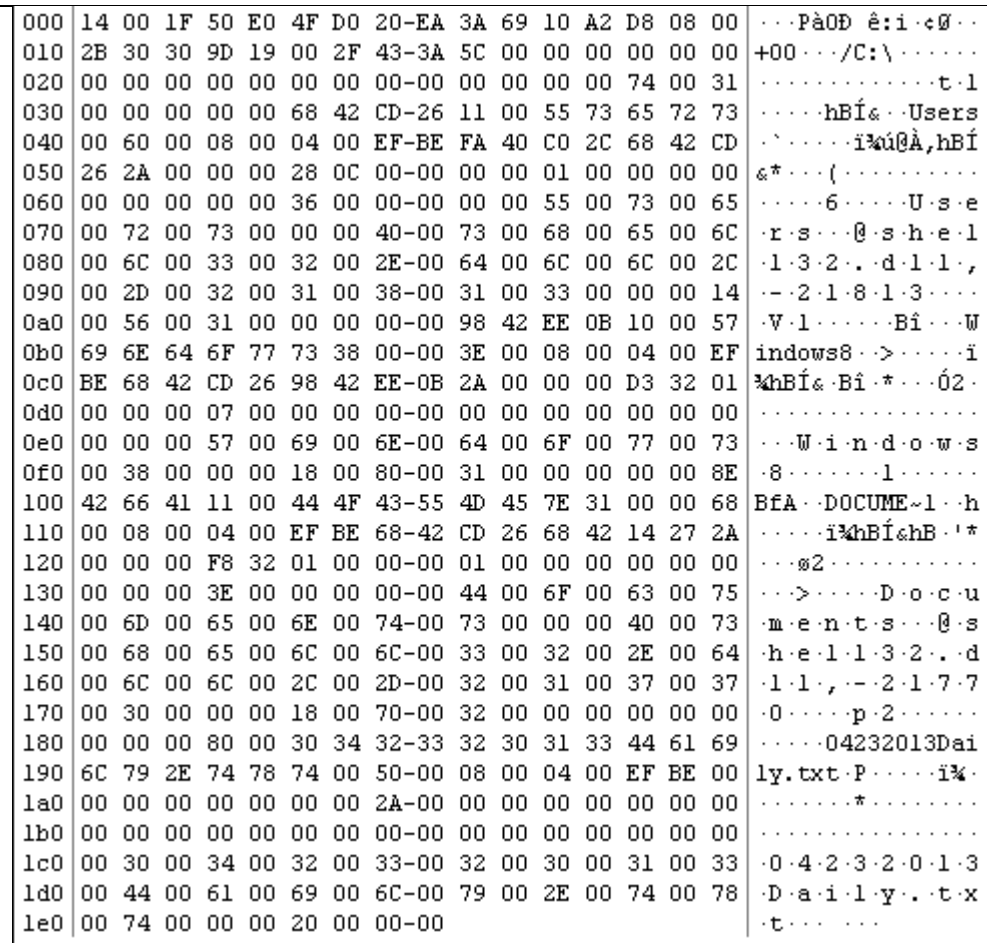
When we explore the registry key NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\ComDlg32\OpenSavePIDlMRU we are able to see a listing of files that have recently been opened or saved:



Name	Type	Data
MRUListEx	REG_BINARY	13 00 00 00 12 00 00 00 11 00 00 00 10 00 00 00 0F 00 00 00 0E 00 00 00 0D 00 00 00 0C 00 00 00 0B 00 00 00 0A 00 00 00 09 00 00 00 08 0...
19	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
18	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
17	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
16	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
15	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
14	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
13	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
12	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 ...
11	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 ...
10	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 ...
9	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 ...
8	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 ...
7	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
6	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
5	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
4	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
3	REG_BINARY	14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1A 00 EE BB FE 23 00 00 10 00 90 E2 4D 37 3F 12 65 45 91 64 39 ...
2	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
1	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0	REG_BINARY	14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Figure 87 OpenSavePIDlMRU Registry Key

While the data portion of the recently modified files appears in hexadecimal, the Registry Viewer has the ability to convert that into ASCII text. For example, when I select REG_BINARY 0, I can see both the hexadecimal data and ASCII data side by side:



000	14	00	1F	50	E0	4F	D0	20-EA	3A	69	10	A2	D8	08	00	···PàOÐ ê:i·¢Ø··
010	2B	30	30	9D	19	00	2F	43-3A	5C	00	00	00	00	00	00	+00···/C:\·····
020	00	00	00	00	00	00	00	00-00	00	00	00	00	74	00	31	··············t·1
030	00	00	00	00	00	68	42	CD-26	11	00	55	73	65	72	73	·····hBÍ&··Users
040	00	60	00	08	00	04	00	EF-BE	FA	40	C0	2C	68	42	CD	·`·····ï¾ú@À,hBÍ
050	26	2A	00	00	00	28	0C	00-00	00	00	01	00	00	00	00	&*···(··········
060	00	00	00	00	00	36	00	00-00	00	00	55	00	73	00	65	·····6·····U·s·e
070	00	72	00	73	00	00	00	40-00	73	00	68	00	65	00	6C	·r·s···@·s·h·e·l
080	00	6C	00	33	00	32	00	2E-00	64	00	6C	00	6C	00	2C	·l·3·2·.·d·l·l·,
090	00	2D	00	32	00	31	00	38-00	31	00	33	00	00	00	14	·-·2·1·8·1·3····
0a0	00	56	00	31	00	00	00	00-00	98	42	EE	0B	10	00	57	·V·1·····Bî···W
0b0	69	6E	64	6F	77	73	38	00-00	3E	00	08	00	04	00	EF	indows8··>·····ï
0c0	BE	68	42	CD	26	98	42	EE-0B	2A	00	00	00	D3	32	01	¾hBÍ&·Bî·*···Ó2·
0d0	00	00	00	07	00	00	00	00-00	00	00	00	00	00	00	00	··············
0e0	00	00	00	57	00	69	00	6E-00	64	00	6F	00	77	00	73	···W·i·n·d·o·w·s
0f0	00	38	00	00	00	18	00	80-00	31	00	00	00	00	00	8E	·8·····l·····
100	42	66	41	11	00	44	4F	43-55	4D	45	7E	31	00	00	68	BfA··DOCUME~l··h
110	00	08	00	04	00	EF	BE	68-42	CD	26	68	42	14	27	2A	·····ï¾hBÍ&hB·'*
120	00	00	00	F8	32	01	00	00-00	01	00	00	00	00	00	00	···ø2··········
130	00	00	00	3E	00	00	00	00-00	44	00	6F	00	63	00	75	···>·····D·o·c·u
140	00	6D	00	65	00	6E	00	74-00	73	00	00	00	40	00	73	·m·e·n·t·s···@·s
150	00	68	00	65	00	6C	00	6C-00	33	00	32	00	2E	00	64	·h·e·l·l·3·2·.·d
160	00	6C	00	6C	00	2C	00	2D-00	32	00	31	00	37	00	37	·l·l·,·-·2·1·7·7
170	00	30	00	00	00	18	00	70-00	32	00	00	00	00	00	00	·0·····p·2·····
180	00	00	00	80	00	30	34	32-33	32	30	31	33	44	61	69	·····04232013Dai
190	6C	79	2E	74	78	74	00	50-00	08	00	04	00	EF	BE	00	ly.txt·P·····ï¾·
1a0	00	00	00	00	00	00	00	2A-00	00	00	00	00	00	00	00	·······*········
1b0	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	··············
1c0	00	30	00	34	00	32	00	33-00	32	00	30	00	31	00	33	·0·4·2·3·2·0·1·3
1d0	00	44	00	61	00	69	00	6C-00	79	00	2E	00	74	00	78	·D·a·i·l·y·.·t·x
1e0	00	74	00	00	00	20	00	00-00								·t··· ···

Figure 88 HEX and ASCII Data REG_BINARY 0 OpenSavePIDIMRU

This is the case for every item within the OpenSavePIDIMRU. Using this ability I can see the most recently opened or saved files. From this we can see that the following names correspond to the following applications:

Table 14 OpenSavePIDIMRU Applications

Name	Application in Text
19	05042013Daily.txt.txt
18	05032013Deleted.txt.txt
17	05032013Attachment.txt
16	05032013Daily.txt.txt
15	05012013attachment.txt
14	05012013Deleted.txt
13	05012013Daily.txt
12	Rit_alum_assoc.jpg
11	Tiger_walking_rit_color.jpg
10	Tiger_walking.jpg
9	Rit_white_no_bar.jpg

8	Rit_black_no_bar.jpg
7	04282013deleted.txt
6	04282013daily.txt
5	04262013daily.txt
4	04252013daily.txt
3	README.txt
2	04242013attachment.txt
1	04242013deleted.txt
0	04232013daily.txt

When we explore the registry key NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\ComDlg32\LastVisitedMRU we are able to see a listing of applications that were recently used to open or save the files listed in the OpenSavePIDIMRU registry key:

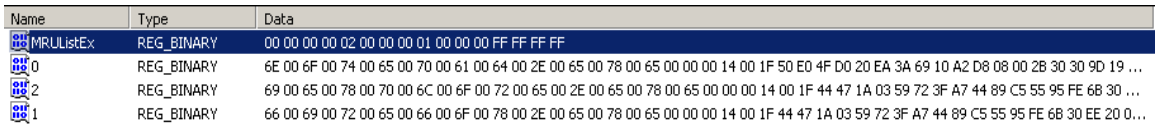


Figure 89 LastVisitedPidMRU Registry Key

As was the case with the previous registry key, the data portion appears in hexadecimal but Registry Viewer can convert that into ASCII text:

```
000 6E 00 6F 00 74 00 65 00-70 00 61 00 64 00 2E 00 n·o·t·e·p·a·d·.·
010 65 00 78 00 65 00 00 00-14 00 1F 50 E0 4F D0 20 e·x·e·····PàOÐ
020 EA 3A 69 10 A2 D8 08 00-2B 30 30 9D 19 00 2F 43 ê:i·¢Ø··+00···/C
030 3A 5C 00 00 00 00 00 00-00 00 00 00 00 00 00 00 :\··············
040 00 00 00 00 00 74 00 31-00 00 00 00 00 68 42 CD ·····t·1·····hBÍ
050 26 11 00 55 73 65 72 73-00 60 00 08 00 04 00 EF &··Users·`·····ï
060 BE FA 40 C0 2C 68 42 CD-26 2A 00 00 00 28 0C 00 ¾ú@À,hBÍ&*···(··
070 00 00 00 01 00 00 00 00-00 00 00 00 00 36 00 00 ·············6··
080 00 00 00 55 00 73 00 65-00 72 00 73 00 00 00 40 ···U·s·e·r·s···@
090 00 73 00 68 00 65 00 6C-00 6C 00 33 00 32 00 2E ·s·h·e·l·l·3·2·.
0a0 00 64 00 6C 00 6C 00 2C-00 2D 00 32 00 31 00 38 ·d·l·l·,·-·2·1·8
0b0 00 31 00 33 00 00 00 14-00 56 00 31 00 00 00 00 ·1·3·····V·1····
0c0 00 98 42 EE 0B 10 00 57-69 6E 64 6F 77 73 38 00 ··Bî···Windows8·
0d0 00 3E 00 08 00 04 00 EF-BE 68 42 CD 26 98 42 EE ·>·····i¾hBÍ&·Bî
0e0 0B 2A 00 00 00 D3 32 01-00 00 00 07 00 00 00 00 ·*···Ó2······
0f0 00 00 00 00 00 00 00 00-00 00 00 57 00 69 00 6E ···········W·i·n
100 00 64 00 6F 00 77 00 73-00 38 00 00 00 18 00 80 ·d·o·w·s·8·····
110 00 31 00 00 00 00 00 8E-42 66 41 11 00 44 4F 43 ·1·····BfA··DOC
120 55 4D 45 7E 31 00 00 68-00 08 00 04 00 EF BE 68 UME~1··h·····i¾h
130 42 CD 26 68 42 14 27 2A-00 00 00 F8 32 01 00 00 BÍ&hB·'*···ø2···
140 00 01 00 00 00 00 00 00-00 00 00 3E 00 00 00 00 ···········>····
150 00 44 00 6F 00 63 00 75-00 6D 00 65 00 6E 00 74 ·D·o·c·u·m·e·n·t
160 00 73 00 00 00 40 00 73-00 68 00 65 00 6C 00 6C ·s···@·s·h·e·l·l
170 00 33 00 32 00 2E 00 64-00 6C 00 6C 00 2C 00 2D ·3·2·.·d·l·l·,·-
180 00 32 00 31 00 37 00 37-00 30 00 00 00 18 00 00 ·2·1·7·7·0·····
190 00                                              ·
```

Figure 90 HEX and ASCII Data REG_BINARY 0 LastVisitedMRU

From this we can see that the following names correspond to the following applications:

Table 15 LastVisitedPidMRU Applications

Name	Application in Text
2	Iexplore.exe
1	Firefox.exe
0	Notepad.exe

When we explore the registry key NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\RecentDocs we are able to see a listing of files and folders that were recently opened:

Figure 91 RecentDocs Registry Key

As was the case with the previous registry key, the data portion appears in hexadecimal but Registry Viewer can convert that into ASCII text:

```
00 6D 00 61 00 69 00 6C 00-2E 00 6C 00 69 00 76 00 m·a·i·l·.·l·i·v·
10 65 00 2E 00 63 00 6F 00-6D 00 2F 00 00 00 86 00 e·.·c·o·m·/·····
20 32 00 00 00 00 00 00 00-00 00 00 00 68 74 74 70 2···········http
30 2D 2D 6D 61 69 6C 2E 6C-69 76 65 2E 63 6F 6D 2D --mail.live.com-
40 2E 6C 6E 6B 00 00 5E 00-08 00 04 00 EF BE 00 00 .lnk··^·····ï¾··
50 00 00 00 00 00 00 2A 00-00 00 00 00 00 00 00 00 ·····*·········
60 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
70 68 00 74 00 74 00 70 00-2D 00 2D 00 6D 00 61 00 h·t·t·p·-·-·m·a·
80 69 00 6C 00 2E 00 6C 00-69 00 76 00 65 00 2E 00 i·l·.·l·i·v·e·.·
90 63 00 6F 00 6D 00 2D 00-2E 00 6C 00 6E 00 6B 00 c·o·m·-·.·l·n·k·
a0 00 00 28 00 00 00                               ··(···
```

Figure 92 HEXl and ASCII Data REG_BINARY 0 RecentDocs Registry Key

From this we can see that the following names correspond to the following applications:

Table 16 RecentDocs Applications

Name	Application in Text
19	05012013attachment.lnk
18	05022013Daily.txt.lnk

17	05012013Daily.lnk
16	http--www.facebook.com-profile.phpid=144008272327176.lnk
15	Rit_alum_assoc.lnk
14	Tiger_walking_rit_color.lnk
13	Tiger_walking_rit.lnk
12	Rit_white_no_bar.lnk
11	Rit_black_no_bar.lnk
10	04282013Deleted.lnk
9	04282013Daily.lnk
7	http--www.facebook.com-photo-phpfbid=10151345109771930&set=a.167899601929.129472.12355161929&type=1.lnk
6	05042013daily.txt.lnk
5	Downloads.lnk
4	05032013attachment.lnk
3	05032013daily.txt.lnk
2	05032013Deleted.txt.lnk
1	05022013Deleted.lnk
0	http--mail.live.com-.lnk

System Hive

The Windows 8 System hive (SYSTEM.dat) found within the C:\Windows\System32\ Config directory as SYSTEM.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 8 virtual machine.

When we explore the registry key SYSTEM.dat\ControlSet001\Control\TimeZoneInformation we are able to see information pertaining to the time zone of the Windows 8 virtual machine. This information is especially useful to forensic investigators as all timestamps within files on this computer are based off of this information:

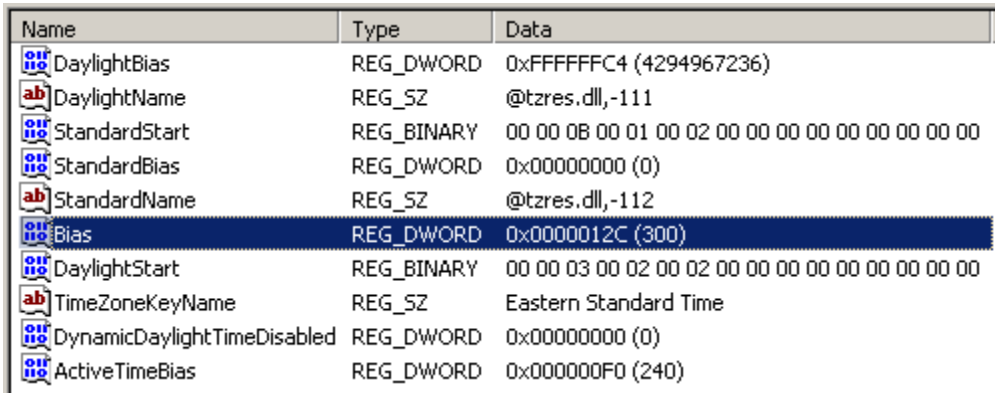
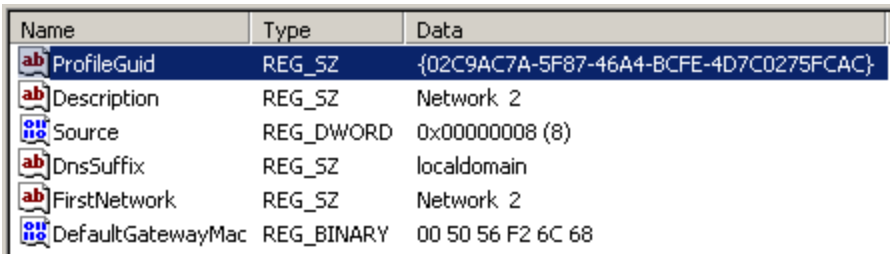


Figure 93 TimeZoneInformation Registry Key

Software

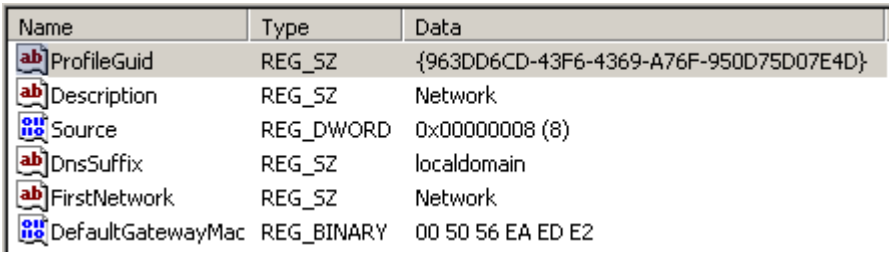
The Windows 8 Software hive (SOFTWARE.dat) found within the C:\Windows\System 32\Config directory as SOFTWARE.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 8 virtual machine.

When we explore the registry key SOFTWARE.dat\ Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged we are able to see information pertaining to the network history of the Windows 8 virtual machine:



Name	Type	Data
ProfileGuid	REG_SZ	{02C9AC7A-5F87-46A4-BCFE-4D7C0275FCAC}
Description	REG_SZ	Network 2
Source	REG_DWORD	0x00000008 (8)
DnsSuffix	REG_SZ	localdomain
FirstNetwork	REG_SZ	Network 2
DefaultGatewayMac	REG_BINARY	00 50 56 F2 6C 68

Figure 94 Unmanaged Network 2 Registry Key



Name	Type	Data
ProfileGuid	REG_SZ	{963DD6CD-43F6-4369-A76F-950D75D07E4D}
Description	REG_SZ	Network
Source	REG_DWORD	0x00000008 (8)
DnsSuffix	REG_SZ	localdomain
FirstNetwork	REG_SZ	Network
DefaultGatewayMac	REG_BINARY	00 50 56 EA ED E2

Figure 95 Unmanaged Network Registry Key

From this we can identify networks that the virtual machine has been connected to. We can also identify important details such as domain name, SSID, and gateway MAC address.

In addition to the Unmanaged registry key, there are additional registry keys that also contain information about network history. In the case of the Windows 8 virtual machine, these keys had no information: SOFTWARE.dat\Microsoft\Windows NT\CurrentVersion\NetworkList \Signatures\Managed.

SAM

The Windows 8 Security Accounts Manager (SAM) hive (SAM.dat) found within the C:\Windows\System32\Config directory as SAM.dat contains a significant amount of information pertaining to the activities of the user created for data generation on the Windows 8 virtual machine.

When we explore the registry key SAM.dat\Domains\Accounts\Users we are able to see a listing of the users that exist on the Windows 8 virtual machine including the administrator, guest, and Windows8 accounts. From this key we can see quite a bit of useful information relating to this user. Information like last logon time, last password change time, invalid logon count, last failed logon time, and many others:

Key Properties	
Last Written Time	4/21/2013 20:04:35 UTC
SID unique identifier	1001
User Name	Windows8
Full Name	Peter Wilson
Logon Count	9
Last Logon Time	4/21/2013 20:04:31 UTC
Last Password Change Time	4/21/2013 20:04:35 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	false
Country Code	1 (United States)
Hours Allowed	Anytime
Has LAN Manager Password	false
Has NTLMv2 Password	true

Figure 96 Users Registry Key

Conclusion

This document explores forensic artifacts including creation/deletion, web browsing, social media, email and the Windows registry. Using both FTK and EnCase, I was able to uncover a majority of the user data that was generated. This serves as a detailed report of the forensic findings made while examining the Windows 8 virtual machine to be included within the appendix of my thesis and later used in a forensic comparison of Windows 7 and Windows 8.

Bibliography

[1] S. Sinofsky, "Releasing Windows 8 - August 1, 2012," Microsoft, 1 August 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/08/01/releasing-windows-8-august-1-2012.aspx. [Accessed 3 April 2013].

[2] S. Sinofsky, "Welcome to Windows 8 – The Consumer Preview," Microsoft, 29 February 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/02/29/welcome-to-windows-8-the-consumer-preview.aspx. [Accessed 3 April 2013].

[3] T. Warren, "Windows 8 Start button removed by Microsoft in 'Consumer Preview'," The Verge, 5 February 2012. [Online]. Available: http://www.theverge.com/microsoft/2012/2/5/2768471/windows-8-start-button-removed-consumer-preview. [Accessed 3 April 2013].

[4] S. Sinofsky, "Creating the Windows 8 user experience," Microsoft, 18 May 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/05/18/creating-the-windows-8-user-experience.aspx. [Accessed 4 Apirl 2013].

[5] S. Sinofsky, "The People app: the complete, cloud-powered address book for Windows 8," Microsoft, 13 June 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/06/13/the-people-app-the-complete-cloud-powered-address-book-for-windows-8.aspx. [Accessed 3 Apirl 2013].

[6] S. Sinofsky, "Web browsing in Windows 8 Release Preview with IE10," Microsoft, 1 June 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/06/01/web-browsing-in-windows-8-release-preview-with-ie10.aspx. [Accessed 4 April 2013].

[7] S. Sinofsky, "Signing in to Windows 8 with a Windows Live ID," Microsoft, 26 September 2011. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2011/09/26/signing-in-to-windows-8-with-a-windows-live-id.aspx. [Accessed 4 April 2013].

[8] S. Sinofsky, "Cloud services for Windows 8 and Windows Phone: Windows Live, reimagined," Microsoft, 2 May 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/05/02/cloud-services-for-windows-8-and-windows-phone-windows-live-reimagined.aspx. [Accessed 4 April 2013].

[9] S. Sinofsky, "Protecting user files with File History," Microsoft, 10 July 2012. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2012/07/10/protecting-user-files-with-file-history.aspx. [Accessed 4 April 2013].

[10] A. C. F. Thomson, "Windows 8 Forensic Guide," Washington, D.C., 2012.

[11] E. Fleisher, "Windows 8 Forensics," 2012.

[12] R. Lee and SANS DFIR Faculty, June 2012. [Online]. Available: http://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf.

[13] J. P. Craiger, "Computer Forensics Procedures and Methods," in *Handbook of Information Security*, Hoboken, NJ, Wiley, 2005, p. 3366.

[14] J. Brunty, "Windows 8 A Forensic First Look," 2012.

[15] K. Johnson, "Windows 8 Forensic Overview," 2012.

[16] R. Lee, "Windows 7 Computer Forensics," 2009.

[17] N. Sofer, 2013. [Online]. Available: http://www.nirsoft.net/utils/hash_my_files.html.

[18] I. Pavlov, 2013. [Online]. Available: http://www.7-zip.org/.

[19] S. Sinofsky, "Delivering fast boot times in Windows 8," Microsoft, 8 September 2011. [Online]. Available: http://blogs.msdn.com/b/b8/archive/2011/09/08/delivering-fast-boot-times-in-windows-8.aspx. [Accessed 4 April 2013].