Rochester Institute of Technology

RIT Digital Institutional Repository

Theses

11-5-2013

A Forensic Comparison: Windows 7 and Windows 8

Peter J. Wilson

Follow this and additional works at: https://repository.rit.edu/theses

Part of the Information Security Commons

Recommended Citation

Wilson, Peter J., "A Forensic Comparison: Windows 7 and Windows 8" (2013). Thesis. Rochester Institute of Technology. Accessed from

This Thesis is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.

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. WilsonThesis 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

Introduction1
Literature Review
Methodology
Network Topology
Virtual Machine Settings
Windows 79
Windows 89
Installed Software
User Data10
Accounts 11
Data Generation
Forensic Analysis14
Data Collection14
Data Preservation
Data Analysis
Reporting19
Results and Comparison
File Creation and Deletion Artifacts
Similarities:
Differences:
Web Browsing Artifacts
Similarities:
Differences:
Social Media Artifacts
Similarities:

Differences:	
Email Artifacts	
Similarities:	
Differences:	
Registry Artifacts	
Similarities:	
Differences:	
Related Works Findings	24
Future Work	27
Conclusion	
Appendices	29
Appendix A: User Data Log	
Appendix B: Windows 7 Forensic Report	
Appendix C: Windows 8 Forensic Report	71
Bibliography	101

List of Tables

Table 1 Virtual Machine Software	10
Table 2 Accounts Created for Virtual Machines	11
Table 3 Windows 7 Data Generation Activities	12
Table 4 Windows 8 Data Generation Activities	13
Table 5 Initial Hash Calculations	15
Table 6 Hash Calculations after Transfer	17
Table 7 Hash Calculations after Forensic Analysis	18
Table 8 Thomson's Local Folder Differences	25
Table 9 Thomson's Windows 8 Registry Differences	25
Table 10 Fleisher's Internet Cookies and History File Location Differences	26

Table 11 OpenSavePIDIMRU Applications	. 65
Table 12 LastVisitedPidMRU Applications	. 66
Table 13 RecentDocs Applications	. 67
Table 14 OpenSavePIDIMRU Applications	. 95
Table 15 LastVisitedPidMRU Applications	. 97
Table 16 RecentDocs Applications	. 97

List of Figures

Figure 1 Entire Network Topology7
Figure 2 Forensic Network Topology
Figure 3 Windows 7 Virtual Machine Settings
Figure 4 Windows 8 Virtual Machine Settings
Figure 5 Uncompressed Virtual Machines Folder 16
Figure 6 Compressed Virtual Machines Folder 16
Figure 7 Johnson's Refresh and Recovery Differences
Figure 8 Windows 7 Created Documents
Figure 9 Windows 7 Created File
Figure 10 Windows 7 Created File
Figure 11 Windows 7 Recovered Deleted Files 43
Figure 12 Recovered File \$RERBVFG.txt
Figure 13 Recovered File \$IERBVFG.txt
Figure 14 Internet Explorer History
Figure 15 Internet Explorer Bookmarks 44
Figure 16 Internet Explorer Cache
Figure 17 Internet Explorer Cached Images
Figure 18 Firefox History
Figure 19 Firefox Favorites
Figure 20 Firefox Cache
Figure 21 Firefox Cached Images
Figure 22 Firefox Stored Login Data
Figure 23 Chrome History 50

Figure 24 Chrome Top Sites	50
Figure 25 Chrome Cache	51
Figure 26 Chrome Cached Images	51
Figure 27 Chrome Login Data	52
Figure 28 Chrome Login Data	53
Figure 29 Social Media Items	54
Figure 30 Windows 7 IEF Case Summary	57
Figure 31 Windows 7 Facebook Activity	58
Figure 32 Windows 7 Twitter Activity	58
Figure 33 Windows 7 Facebook URLs	59
Figure 34 IEF Timeline for Social Media Items	60
Figure 35 IEF Timeline for Social Media Items with Details	60
Figure 36 Email sent to peterwilson.win7@gmail.com	61
Figure 37 Email sent to peterwilson.win7@live.com	62
Figure 38 Email sent from peterwilson.win7@gmail.com	62
Figure 39 Email sent from peterwilson.win7@live.com	63
Figure 40 Forwarded Emails	63
Figure 41 Replied Emails	64
Figure 42 Recovered Email with Attachments	65
Figure 43 OpenSavePIDIMRU Registry Key	65
Figure 44 HEX and ASCII Data REG_BINARY 0 OpenSavePIDIMRU	65
Figure 45 LastVisitedPidMRU Registry Key	66
Figure 46 HEX and ASCII Data REG_BINARY 0 LastVisitedMRU	66
Figure 47 RecentDocs Registry Key	67
Figure 48 HEX and ASCII Data REG_BINARY 0 RecentDocs Registry Key	67
Figure 49 TimeZoneInformation Registry Key	68
Figure 50 Unmanaged Network 2 Registry Key	68
Figure 51 Unmanaged Network Registry Key	69
Figure 52 Users Registry Key	69
Figure 53 Windows 8 Created Documents	71
Figure 54 Windows 8 Created File	71

Figure 55 Windows 8 Created File	71
Figure 56 Windows 8 Recovered Deleted Files	72
Figure 56 Recovered File \$RFGBREV.txt	72
Figure 57 Recovered File \$IFGBREV.txt	72
Figure 58 Internet Explorer and Internet Explorer App History	73
Figure 59 Internet Explorer and Internet Explorer App Bookmarks	73
Figure 60 Firefox History	74
Figure 61 Firefox Favorites	74
Figure 62 Firefox Cache	75
Figure 63 Firefox Cached Images	76
Figure 64 Firefox Stored Login Data	77
Figure 65 Chrome History	78
Figure 66 Chrome Top Sites	78
Figure 67 Chrome Cache	79
Figure 68 Chrome Cached Images	80
Figure 69 Chrome Login Data	81
Figure 70 Chrome Login Data	82
Figure 71 Social Media Items	82
Figure 72 Windows 8 IEF Case Summary	86
Figure 73 Windows 8 Facebook Activity	87
Figure 74 Windows 8 Twitter Activity	87
Figure 75 Windows 8 Facebook URLs	88
Figure 76 IEF Timeline for Social Media	89
Figure 77 IEF Timeline for Social Media Items with Details	89
Figure 78 Email sent to peterwilson.win8@gmail.com	90
Figure 79 Email sent to peterwilson.win8@live.com	91
Figure 80 Email sent from peterwilson.win8@gmail.com	91
Figure 81 Email sent from peterwilson.win8@live.com	92
Figure 82 Forwarded Emails	92
Figure 83 Replied Emails	92
Figure 84 Email Attachments	93

Figure 85 Recovered Email with Attachments	93
Figure 86 OpenSavePIDIMRU Registry Key	94
Figure 87 HEX and ASCII Data REG_BINARY 0 OpenSavePIDIMRU	95
Figure 88 LastVisitedPidMRU Registry Key	96
Figure 89 HEX and ASCII Data REG_BINARY 0 LastVisitedMRU	96
Figure 90 RecentDocs Registry Key	97
Figure 91 HEXI and ASCII Data REG_BINARY 0 RecentDocs Registry Key	97
Figure 92 TimeZoneInformation Registry Key	98
Figure 93 Unmanaged Network 2 Registry Key	99
Figure 94 Unmanaged Network Registry Key	99
Figure 95 Users Registry Key	100

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

Ne	w Virtual Machine	Wizard	X		
	Ready to Create Virtual Machine Click Finish to create the virtual machine and start installing Windows 7 x64 and then VMware Tools.				
	The virtual machine v	vill be created with the following settings:			
	Name:	Windows 7			
	Location:	P:\Virtual Machines\Windows 7			
	Version:	Workstation 9.0			
	Operating System:	Windows 7 x64			
	Hard Disk:	d Disk: 40 GB, Pre-allocated			
	Memory:	1024 MB			
	Network Adapter:	NAT	_		
	•)			
	Customize Hardw.	are ual machine after creation			
		< Back Finish Cance			

Figure 3 Windows 7 Virtual Machine Settings

Windows 8

Nev	ew Virtual Machine Wizard 🛛 🛛 🗙				
	Ready to Create Virtual Machine Click Finish to create the virtual machine and start installing Windows 8 x64 and then VMware Tools.				
	The virtual machine will be created with the following settings:				
	Name:	Windows 8			
	Location:	P:\Virtual Machines\Windows 8			
	Version:	Workstation 9.0			
	Operating System:	: Windows 8 x64			
	Hard Disk:	40 GB, Pre-allocated			
	Memory:	1024 MB			
	Network Adapter:	Adapter: NAT			
Customize Hardware					
	< Back Finish Cancel				

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.

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

Table I virtual machine poleward	Table 1	Virtual	Machine	Software
----------------------------------	---------	---------	---------	----------

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.

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:
facebook.com/windowsseven.forensics	facebook.com/windowseight.forensics
Twitter:	Twitter:
twitter.com/win7forensics	twitter.com/win8forensics

Table 2 Accounts Created for	r Virtual Machines
-------------------------------------	--------------------

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 <u>Appendix A</u>).

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\		×		×	×	×	×	×	×	
Created Attachment File in C:\Users\Windows7\Documents\			×				×		×	
Created Deleted File in C:\Users\Windows7\Documents\			×			×	×		×	
Downloaded File to C:\Users\Windows7\Downloads\		×		×	×		×		×	
Deleted File in C:\Users\Windows7\Documents\			×			×	×	×	×	
Deleted File in C:\Users\Windows7\Downloads\				×			×		×	×
Empty the Recycle Bin					×					×
Browsed to the Featured Wikipedia Article using all Browsers	×	×	×	×	×	×	×	×	×	×
Browsed to RIT's Top News Stories for the day using all Browsers	×	×	×	×	×	×	×	×	×	×
Browsed to Facebook, Automatically Logged In using all Browsers	×	×	×	×	×	×	×	×	×	×
Browsed to Twitter, Automatically Logged In using all Browsers	×	×	×	×	×	×	×	×	×	×
Sent email to other 3 accounts from the Windows7 Live Account	×				×					
Sent email to other 3 accounts from the Windows7 Gmail Account		×		×				×		×
Sent email with attachments to other 3 accounts from the Windows7 Live Account			×				×		×	
Sent email with attachments to other 3 accounts from the Windows7 Gmail Account						×				
Reply to Daily Email using Windows Live Mail 2012 to Original Sender				×	×		×		×	
Forward Daily Email using Windows Live Mail 2012 to Original Sender				×	×		×		×	
Posted Daily Post on Facebook	c	п	Ē	c	т	m	C	т	m	E
Shared Post of Facebook	E	C	п		C	Ŧ				п
Shared Photo on Facebook				m			Ē	C	т	
Comment on Daily Facebook Post				С	'n	m	C	т	m	Ē
Like Daily Facebook Post					п	m	C	т	m	雨
Tweeted Daily Tweet on Twitter	п	Ē	C	т	m	C	п	m	c	C
Retweeted Tweet on Twitter		E	C	т	m	C	т	m	c	C
Reply to Daily Tweet on Twitter				m	c	т	m	C	т	т
Checked for Updates			×	×			×		×	×
Installed Important Updates										
Table										
C = Chrome										
IE = Internet Explorer										
IE App = Internet Explorer App										
F = Firefox										

Table 3 Windows 7 Data Generation Activities

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

Table 4 Windows 8 Data Generation Activities

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 7flat.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:

Filename	MD5	SHA1	SHA-256	Full Path	Modified Time	Created Time	File Size
Windows 7- flat.vmdk	8800bcad1a 173fd07a1b 74f11c8545 b9	81290ce98 9246c28d1 40092a46f 60e1e91d 1d89f	71d09c22 80225235 d18b30f55 99ae37fef 4d2f38a98 499c615f0 5fc6632e2 f11	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	752594eab 4acf342891 d7fe4421e4 777	9ca91f650 de285d2af 8f863b1c2 efeee7310 ea34	3643019d 5ed03d6e e4a24518 3e3897eb 665a0d39 2dbf5504a 4b51f346b dfefaa	F:\Virtual Machines\ Windows 8\Windows 8-flat.vmdk	5/4/2013 3:59:25 PM	5/7/2013 9:51:52 AM	42949672960

Table 5 Initial Hash Calculations

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:

Jirtual Mach	nines Properties X	General Secu	nines.72 Properties 🛛 🗙
1	Virtual Machines		Virtual Machines.7z
Type: Location:	File folder P:\\	Type of file: Opens with:	7Z File (.7z) Windows Shell Commor Change
Size: Size on disk: Contains:	80.0 GB (85,906,641,639 bytes) 80.0 GB (85,907,636,224 bytes) 346 Files 10 Folders	Location: Size: Size on disk:	0:\ 17.1 GB (18,363,242,840 bytes) 17.1 GB (18,363,244,544 bytes)
Created:	Thursday, March 07, 2013, 1:32:37 PM	Created: Modified:	Sunday, May 05, 2013, 12:29:38 AM Sunday, May 05, 2013, 10:47:21 AM
Attributes:	Bead-only (Only applies to files in folder) Hidden Advanced	Accessed: 	Sunday, May 05, 2013, 12:29:38 AM
	OK Cancel Apply		OK Cancel Apply

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:

Filename	MD5	SHA1	SHA-256	Full Path	Modified	Created	File Size
	8800bcad1a	81290ce98	71d09c22 80225235 d18b30f55	F:\Virtual	Time	Time	
Windows 7- flat.vmdk	173fd07a1b 74f11c8545 b9	40092a46f 60e1e91d 1d89f	99ae37fef 4d2f38a98 499c615f0 5fc6632e2 f11	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	752594eab 4acf342891 d7fe4421e4 777	9ca91f650 de285d2af 8f863b1c2 efeee7310 ea34	3643019d 5ed03d6e e4a24518 3e3897eb 665a0d39 2dbf5504a 4b51f346b dfefaa	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:

Filename	MD5	SHA1	SHA-256	Full Path	Modified Time	Created Time	File Size
Windows 7- flat.vmdk	8800bcad1a 173fd07a1b 74f11c8545 b9	81290ce98 9246c28d1 40092a46f 60e1e91d 1d89f	71d09c22 80225235 d18b30f55 99ae37fef 4d2f38a98 499c615f0 5fc6632e2 f11	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	752594eab 4acf342891 d7fe4421e4 777	9ca91f650 de285d2af 8f863b1c2 efeee7310 ea34	3643019d 5ed03d6e e4a24518 3e3897eb 665a0d39 2dbf5504a 4b51f346b dfefaa	F:\Virtual Machines\ Windows 8\Windows 8-flat.vmdk	5/4/2013 3:59:25 PM	5/7/2013 9:51:52 AM	42949672960

Table 7 Hash Calculations after Forensic Analysis

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
 - o Firefox
 - Chrome
- Social Media Artifacts
 - Facebook Activity
 - o 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 <u>Appendix B</u> and <u>Appendix C</u> 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:

Application	Location	Purpose	
Metro Apps	Microsoft\Windows\Application Shortcuts	Apps that are displayed on the Metro interface	
IF 10 Wateritas Visited	Microsoft\InternetExplorer\Recovery\ Immersive\Active	Wakeitas usas visitad ukila krowsing with IE10	
TE 10 Websites visited	Microsoft\InternetExplorer\Recovery\ Immersive\Last Active	websites user visited while browsing with into.	
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.	

Table 8 Thomson's Local Folder Differences

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:

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%

Table 9 Thomson's Windows 8 Registry Differences
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 Interne	Cookies and History	File Location Differences
-----------------------------	---------------------	----------------------------------

Cooling	<root>\users\<username>\appdata\roaming\</username></root>	<root>\users\<username>\appdata\roaming\</username></root>		
COOKIES	microsoft\windows\cookies\	microsoft\windows\cookies\low		
	<root>\users\<username>\appdata\local\</username></root>	<root>\users\<username>\appdata\local\</username></root>		
Temporary Internet Files	microsoft\microsoft\windows\history	microsoft\microsoft\windows\history		
	contained in index.dat	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 7 and Windows 8 is minimal.

Appendices

Appendix A: User Data Log

04/21/2013	
Window	vs 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.Win	7@live.com
	Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article:
http://en.wikiped	ia.org/wiki/Reginald_Heber
	Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day:
http://www.rit.ed	u/news/story.php?id=49953&source=enewsletter and
http://www.rit.ed	u/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 pas	ssword
	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
Window	vs 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.Win	7@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

 $Created \ File \ C: \ Windows \& Documents \\ 04232013 \\ daily.txt$

04/24/2013

Windows 7 around 9:10PM

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

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

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

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

C	Created File C:\Users\Windows7\Documents\04242013attachment.txt
L	Jsing Mail App, sent email to other 3 accounts from the Live Account with Attached File
04232013attachme	nt.txt
τ	Jsing 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
τ	Jsing 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
L	Jsing IE App, IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In
τ	Jsing IE App, IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In
Γ	Downloaded File http://mirrors.rit.edu/centos/6.4/isos/i386/README.txt to
C:\Users\Windows	8\Downloads folder using Firefox
τ	Jsing Firefox Shared IST at RIT's Post on Facebook about being a TA
U	Jsing Chrome Tweeted Daily Tweet
U	Jsing Chrome Retweeted @RITsports Tweet
U	Jsing IE App Posted Daily Post on Facebook
Γ	Deleted Chrome and Firefox Shortcuts from Desktop
Γ	Delete File C:\Users\Windows8\Documents\04242013deleted.txt at 9:42PM
C	Checked for Updates, Installed 1 Important Update
τ	Jsing Weather App looked at weather for Rochester, NY and Seattle, WA
τ	Jsing Map App, Set home as Rochester Institute of Technology 117 Lomb Memorial Drive,
Rochester, NY	
τ	Jsing 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
C	Created File C:\Users\Windows7\Documents\04252013daily.txt
Ľ	Jsing Windows Live Mail 2012, sent email to other 3 accounts from the Gmail Account
τ	Jsing IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article:
http://en.wikipedia.	.org/wiki/Franco-Mongol_alliance
L L	Jsing 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
L	Jsing IE, Firefox, and Chrome Browsed to Facebook, Auto Logged In
τ	Jsing IE, Firefox, and Chrome Browsed to Twitter, Auto Logged In
τ	Jsing 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://mirro	rs.rit.edu/openoffice/packages/14/OOo_3.3.0_Win_x86_install_om.exe to
C:\Users\W	indows7\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	n.Win7@gmail.com
	Using Windows Live Mail 2012 Forward the Daily Email using Live Account to
PeterWilson	n.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
W	indows 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.wi	kipedia.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://mirro	rs.rit.edu/openoffice/packages/14/OOo_3.3.0_Win_x86_install_om.exe to
C:\Users\W	indows8\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.ed	lu/news/story.php?id=49968&source=enewsletter and
http://www.rit.ed	lu/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 throug	h 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\Window	vs8\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	
Window	vs 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	1
	Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article:
http://en.wikiped	ia.org/wiki/1923_FA_Cup_Final
	Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day:
http://www.rit.ed	lu/news/story.php?id=49972&source=enewsletter and
http://www.rit.ed	lu/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
Window	vs 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	1
	Using IE App, IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article:
http://en.wikiped	ia.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.ed	u/news/story.php?id=49972&source=enewsletter and
http://www.rit.ed	u/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	
Window	vs 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 050	12013attatchment.txt attached
	Using IE, Firefox, and Chrome Browsed to the Featured Wikipedia Article:
http://en.wikiped	ia.org/wiki/If Day
	Using IE, Firefox, and Chrome Browsed to RIT's Top News Stories for the day
	company and containe browsed to fair a reprice as borres 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

 $Created \ File \ C: \ Windows 8 \ Documents \ 0502013 \ daily.txt$

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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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:

 Hex
 Text
 Filtered
 Natural

 00
 54
 68
 69
 73
 20
 69
 73
 20
 74
 65
 76
 74
 This is the text

 10
 20
 66
 69
 62
 52
 74
 65
 76
 74
 This is the text

 10
 20
 66
 69
 62
 52
 63
 72
 65
 64
 20
 67
 6E
 file
 created on
 04/23/2013 at 9
 04/23/2013 at 9
 04/23/2013 at 9
 :55pm

Figure 9 Windows 7 Created File

 Hex
 Text
 Fibered
 Natural

 00
 54
 68
 69
 73
 20
 66
 69
 62
 65
 20
 77
 61
 73
 20
 63
 72
 This file was cr

 10
 65
 61
 74
 65
 64
 20
 6F
 6E-20
 30
 31
 2F
 32
 eated on 05/01/2

 20
 30
 31
 32
 06
 74
 61
 67
 30
 12
 F32
 eated on 05/01/2

 20
 30
 31
 32
 06
 74
 20
 31
 31
 84
 41
 42
 0
 013<at<11:16&//r.</td>

 30
 0A
 49
 74
 20
 77
 46
 63
 68
 64
 11
 was attached

 40
 20
 74
 61
 62
 20
 67
 66
 to and enail on

 50
 20
 73
 31
 27
 30
 31

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: File Created Item Path Name Written Accessed Analysis Type 🐜 \$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 sierbvfg.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: () Fields 🛛 Report 🚵 Text 🔣 Hex 🛗 Decode 📧 Doc 📀 Transcript 🖺 Picture Lock G 💮 Options 🍡 Codepage 👻 🗛 Text Style 👻 👬 Find 🧤 🔚 🔁 📃 💷 Compressed View 📑 Previous Item 🛄 Next Item 20 3 68 69 73 20 66 69 6C 65 20 77 61 73 20 63 72 65 61 74 65 64 20 67 68 20 30 34 27 32 38 27 32 30 31 33 20 61 74 20 33 3A 34 30 anis file was created on 04/28/2013 at 3:40 Figure 12 Recovered File \$RERBVFG.txt The second file, \$IERBVFG.txt has the following contents: () Fields 🐱 Report 🎦 Text 🧱 Hex 🎬 Decode 📧 Doc 📳 Transcript 🖺 Picture 🗆 Lock 🛛 🔁 😓 Options 🍡 Codepage 💌 🗛 Text Style 💌 🌺 Find 斗 📑 📜 💷 Compressed View 📑 Previous Item 📃 Next Item
 Corpusors
 Contensions
 ·U ``¤RDηC·:·∖·U·s·e·r·s 1 ws·7·\.D·o·c·u·m·e·n·t·s·\.O· 3-d·e·1·e·t·e·d·..·t·x·t·..·t·x·t

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	Uri 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	Histon/Typed URL
Internet Explorer (Windows)	url8	05/01/13 11:30:55AM	http://www.rit.edu/news/nandedaily.php	Windows7	Histon/Typed URL
Internet Explorer (Windows)	url9	05/01/13 11:30:55AM	http://en.wikipedia.org/wiki/Main_Page	Windows7	Histon/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	Histon/Typed URL
Internet Explorer (Windows)	url4	05/01/13 11:30:55AM	http://live.com/	Windows7	Histon/Typed URL
Internet Explorer (Windows)	url5	05/01/13 11:30:55AM	http://gmail.com/	Windows7	Histon/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	Histon/Typed URL
Internet Explorer (Windows)	url9	05/01/13 11:30:55AM	http://en.wikipedia.org/wiki/Main_Page	Windows7	Histon/Typed URL
Internet Explorer (Windows)	url10	05/01/13 11:30:55AM	http://go.microsoft.com/fwlink/?LinkId=69157	Windows7	Histon/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&rpsrv=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 <u>http://downloads.microsoft.com</u>. I am unsure why this information appears in this location as it would certainly hinder a true forensic investigation:

Browser Type	Uri 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/NeutraIMSU/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/NeutraIMSU/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/NeutraIMSU/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/NeutraIMSU/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/NeutraIMSU/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/SetupPolicv.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:



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	Title	Uri Name	Internet ^
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=Io&jIou=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	Uri 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	ttp://www.rit.edu/imagine/images/featured/poster_winner_2013.jpg	
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	



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	Uri 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 Anne	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:

Chrome (Windows) Chrome (Windows)		Name	Artifact Typ
Chrome (Windows)	05/03/13 04:42:25PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/ys/r/fnBZhAggpcM.png	CacheVImag
	05/04/13 03:40:20PM	http://upload.wikimedia.org/wikipedia/commons/thumb/d/d6/Wikiguote-logo-en.svg/40px-Wikiguote-logo-en	Cache\Imag
Chrome (Windows)	05/04/13 03:40:29PM	https://fbcdn-creative-a.akamaihd.net/hads-ak-ash3/s110x80/735327_6007144937656_507415288_n.png	Cache\Imag
Chrome (Windows)	05/03/13 04:42:19PM	http://www.rit.edu/news/images/blog.gif	Cache\Imag
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/sponsors2010/rghs.gif	Cache\Imag
Chrome (Windows)	05/04/13 03:41:03PM	http://profile.ak.fbcdn.net/hprofile-ak-prn1/48824_732486294_342702120_g.jpg	Cache\Imag
Chrome (Windows)	05/04/13 03:40:07PM	http://meta.wikimedia.org/wiki/Special:RecordImpression?result=hide&reason=empty&country=US&uselang=	Cache∖Imag
Chrome (Windows)	05/04/13 03:40:30PM	https://fbcdn-sphotos-e-a.akamaihd.net/hphotos-ak-ash4/s480x480/485400_10151352916191930_2119440542_n	Cache∖Imag
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/sponsors2011/hp.gif	Cache\Imag
Chrome (Windows)	05/04/13 03:41:00PM	http://farm9.staticflickr.com/8268/8706880044_d355128ec7_s.jpg	Cache\Imag
Chrome (Windows)	05/04/13 03:41:03PM	http://profile.ak.fbcdn.net/hprofile-ak-frc1/275407_100005370100122_1057571410_qjpg	Cache∖Imag
Chrome (Windows)	05/03/13 04:42:23PM	https://twimg0-a.akamaihd.net/sticky/default_profile_images/default_profile_6_mini.png	Cache∖Imag
Chrome (Windows)	05/04/13 03:40:15PM	http://upload.wikimedia.org/wikipedia/en/b/bc/Wiki.png	Cache\Imag
Chrome (Windows)	05/03/13 04:43:12PM	http://www.rit.edu/news/lib/filelib/201305/smithtaylor.jpg	Cache\Imag
Chrome (Windows)	05/03/13 04:42:24PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/y9/r/jKEc/PZFk-2.gif	Cache\Imag
Chrome (Windows)	05/03/13 04:42:26PM	https://www.facebook.com/images/spacer.gif	Cache∖Imag
Chrome (Windows)	05/03/13 04:42:18PM	http://www.rit.edu/news/images/daily/header-20130503.jpg?1882678350	Cache∖Imag
Chrome (Windows)	05/03/13 04:42:26PM	https://fbstatic-a.akamaihd.net/rsrc.php/v2/yA/r/4WSewcWboV8.png	Cache\Imag
Chrome (Windows)	05/02/13 03:14:24PM	http://l.yimg.com/a/i/us/we/52/28.gif	Cache\Imag
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/nav-right.gif	Cache∖Imag
Chrome (Windows)	05/03/13 04:43:12PM	http://www.rit.edu/news/lib/filelib/201305/pancarischott.jpg	Cache\Imag
Chrome (Windows)	05/03/13 04:42:28PM	https://fbcdn-profile-a.akamaihd.net/hprofile-ak-frc1/s32x32/275407_100005370100122_1057571410_q.jpg	Cache\Imag
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\Imag
Chrome (Windows)	05/03/13 04:42:18PM	http://www.rit.edu/_files/bodyBG.gif	Cache\Imag
Chrome (Windows)	05/04/13 03:40:58PM	http://www.rit.edu/imagine/images/2012-header.gif	Cache\Imag
Chrome (Windows)	05/03/13 04:42:24PM	http://www.rit.edu/_files/footer.gif	CacheVimag
l during the da	ata generation p	process:	5
Table Timeline	ata generation p Gallery Gallery Gallery Gallery Gallery Gallery (122	Drocess: fore Columns 1122 1122 1122 1123 <th>(1235</th>	(1235
during the da	ata generation p Gallery Gallery Gallery Gallery Gallery Common Gallery Common	fore Columns (122) (122) (122) (. (1235
d during the da	ata generation p Gallery Gallery Gallery Gallery Common Network Common N	Tore Columns (122) (122) (122) (122) (122) (122) (122) (122) (122) (122) (122) (122) (122) (122) (123) (124) (123) (124) (123) (124) (123) (124) (123) (124) (124) (124) (124) (124) (124) (124) (124) (124)	(1235) (1248
during the da	ata generation p Gallery Gallery Fewer Columns IN 22 I (122 I CONSIST 23 I (123 I CONSIST 23 I (123 I CONSIST I (123 I CONSIS	fore Columns (122) (122) (122) (123) (124)) (1235 (1246) (1246)
I during the da	ata generation p Gallery Gallery Fewer Columns N 22 Columns N Columns Colum	fore Columns (122) (122) (122) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (123) (124)	(1248 (1248) (1248) (1261)
during the da Table Timelin Carlor Control (1948) Carlor Control	ata generation p Gallery Fewer Columns I Fewer Columns I I Enver Columns I I Enver Columns I I I I I I I I I I I I I I I I I I I	Arre Columns 122 122 122 123 124 125 <td>) = (1235 </td>) = (1235
d during the da Table Timelin Selected 0/1048 Call 22 Call Call 22 Call 22 Call Call 22 Call 22 Ca	ata generation p Gallery Fewer Columns I Fewer Columns I I Enver Columns I I Enver Columns I I I I I I I I I I I I I I I I I I I	Arree Columns (122) (122) (122) (123) (124) (125) (125) (125) (125) (125) (125) (125) (126) (126) (126) (127) (127) (127) (127) (127) (127) (127) (127) (127) (127) <t< td=""><td>) = (1246) = (1246) = (1246) = (1261) = (1274</td></t<>) = (1246) = (1246) = (1246) = (1261) = (1274

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: 🐴 Home 🛛 📢 Records 🗙 🔇 🟮 🅈 Viewing (Internet) 🔻 🛄 Split Mode 🔻 (ﷺ Condition 👻 🍟 Filter 🖛 🖓 Tags 💌 🎃 Review Package 💌 👧 Bookmark 💌 🛃 Go to file | 🕘 Find Relat 🔺 🖂 🌛 Internet 📰 Table 🛛 🕙 Timeline 🛛 🖺 Gallery -D- Internet Explorer (Windows) 🌶 🏢 👻 🫓 👻 🗔 Selected 0/10483 Chrome (Windows) Browser Url Internet -D🗔 🌡 Cookies Created Type Artifact Type Name 🕒 📙 Login Data Login Data 1 Chrome (Windows) https://twitter.com/ 04/21/13 03:47:43PM -DC bownloads 2 Chrome (Windows) https://twitter.com/ Login Data 04/21/13 03:47:43PM -D-1 History 3 Chrome (Windows) https://twitter.com/ Login Data 04/21/13 03:47:43PM -D🗌 🌡 Top Sites 4 Chrome (Windows) https://twitter.com/ - D Cache Login Data 04/21/13 03:47:43PM 5 Chrome (Windows) https://www.facebook.com/ D 😼 Video Login Data 04/21/13 03:45:52PM – 🕞 🔒 Unknown Type 6 Chrome (Windows) https://www.facebook.com/ Login Data 04/21/13 03:45:52PM D 7 Chrome (Windows) https://www.facebook.com/ Login Data 04/21/13 03:45:52PM -D-3 Code 8 Chrome (Windows) https://www.facebook.com/ Login Data 04/21/13 03:45:52PM D Mozilla (Windows/Mac) DOL Mozilla 3 (Windows/Mac) 4 🐱 Report 🞦 Text 🕮 Hex 🎬 Decode 📧 Doc 📄 Transcript 📳 Picture () Fields $^{\circ}$ Zoom In 🛛 💆 Zoom Out 🍕 100% 🔻 🛅 Previous Item 🛄 Next Item Internet Artifact Login Data Type Url Name https://www.facebook.com/ Url Host www.facebook.com/ Action Url https://www.facebook.com/login.php Username email Element peterwilson.win7@gmail.com User Password Element pass 01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 d0 4f c2 97 eb 01 00 00 00 d6 97 da 84 5a d5 d6 4f 8e Password Value 16 e5 2f 89 3d ae 63 00 00 00 00 02 00 00 00 00 00 10 66 00 00 01 00 00 20 00 00 02 9f2 ee 86 55 53 ad 7b dc be 97 c7 16 3f c1 ae 38 b2 a0 32 31 2c 8c 32 4c a6 18 1f 7b 51 67 48 00 00 00 00 0e 80 00 00 00 02 00 00 20 00 00 00 eb 85 2f 54 b3 09 a6 33 b9 3c 44 06 54 7a 30 b5 13 72 b1 a7 f4 bb e1 c2 a4 d4 b1 60 f3 43 0b 00 10 00 00 d2 84 79 cf ab 32 ad 38 83 a3 bd 23 1f 92 da 69 40 00 00 00 59 83 61 3c 70 c7 3f 0d ec 82 15 95 c7 74 d1 0b 74 96 af df 7c 57 f3 73 6f d0 4f 7d 84 e2 51 36 de 99 89 f2 7e a1 2b 4c ef 9f 4d 46 cd 54 a6 7e 11 4b fc 71 c7 21 de 06 05 0c 0b 5a 64 8e ef 0f Signon Realm https://www.facebook.com/ Ssl Valid Preferred 04/21/13 03:45:52PM Created Blacklisted 0 Scheme 0 Browser Type Chrome (Windows) Profile Name Windows7 Message Size 0 **Figure 27 Chrome Login Data**

	nternet) + E split Mode	▼ [[≣ Condition ▼	🍸 Filter 🔻 🕫 Tags 💌 🤬 Review Package 💌 🚫)Bookmark 🔻 📄	Go to file 🛛 🧕 Find Re
🗕 🕞 🔒 Internet	(m)	Fable 😔 Timeline	E Gallery		
Þ-D-D- 📕 Internet E	xplorer (Windows)		sted 0/10493		
- Chrome (V	Windows)	Descuses	114	Technometh	
-DJ Cookie	5	Type	Name	Artifact Type	Created
Degin L	Data 1	Chrome (Windows)	https://twitter.com/	Login Data	04/21/13 03:47:43PM
-Du Downie	oads	Chrome (Windows)	https://twitter.com/	Login Data	04/21/13 03:47:43PM
- History	3	Chrome (Windows)	https://twitter.com/	Login Data	04/21/13 03:47:43PM
Cache	4	Chrome (Windows)	https://twitter.com/	Login Data	04/21/13 03:47:43PM
Vide		Chrome (Mindows)	https://www.facebook.com/	Login Data	04/21/13 03:45:52PM
	nown Type	Chrome (Alindows)	http://www.facebook.com/	Login Data	04/21/13 03:45:52PM
	ae 7	Chrome (kindows)	https://www.facebook.com/	Login Data	04/21/12 02:45:52PM
		Chrome (Windows)	https://www.facebook.com/	Login Data	04/21/13 03:45:52PM
	1L 8	crirome (windows)	nups://www.facebook.com/	Login Data	04/21/13 03:45:52PM
Report Text Zoom In Text Tope Url Name Url Host Action Url	Hex Decode mout 100% - Pro	🖻 Doc 📄 Transcrip evious Item 🎑 Next	ot 📳 Picture () Fields Item		
Report Text Coom In Coor Internet Artifact Type Url Name Url Host Action Url Username Element	Hex in Decode Hex in Decode Mout in 100% The Pro- Login Data https://twitter.com/ twitter.com/ https://twitter.com/sessi session[username_or_ender]	Doc 📄 Transcrig evious Item 💽 Next ions mail]	ot 🖺 Picture () Fields Item		
Report Text Com In Con Internet Artifact Type Url Name Url Host Action Url Username Element User	Hex in Decode Hex in Decode Mout @ 100% T Pro Login Data https://twitter.com/ twitter.com/ https://twitter.com/sessi session[username_or_et peterwilson.win7@live.co	Doc 📄 Transcrip evious Item 🎑 Next ions mail]	ot 🖺 Picture () Fields Item		
Report Text	Hex min Decode Hex min Decode 100% ▼ Protect Login Data https://twitter.com/ twitter.com/ https://twitter.com/sessis session[username_or_end peterwilson.win7@live.com session[password] 01 00 00 00 d0 8c 9d dr 01 16 e5 2f 89 3d ae 63 00 00 eb e3 55 1d b8 b8 ef 65 com 00 00 00 00 20 00 20 00 00 7d 95 41 9a 3b 67 41 9a 61 00 55 31 5a 74 3a 1b ca 73 22 60 b1 13 95 c6 84 fe 6e	Doc Transcrip evious Item Next lons mail] com 15 dl 11 8c 7a 00 d0 4 00 00 02 00 00 00 00 00 159 0e fc 92 01 b7 d7 00 00 fa 74 d5 76 70 00 00 fa 74 d5 76 70 00 00 fa 74 d5 76 70 1 d6 51 9a ea c2 62 9f 10 60 10 32 36 29 f10 60 10 32 36	picture Fields Item 1 Fields 1 6 0		
Report Text	Hex min Decode Mout	Doc Transcrip evious Item Next ions mail] com 15 dl 11 8c 7a 00 d0 4 00 00 02 00 00 00 00 0 159 0e fc 92 0l b7 d0 00 00 fa 7f ad 5f 6f 00 00 00 fa 51 9 ae ac 2 62 9f 10 60 f0 03 23 6	f c2 97 eb 01 00 00 00 d6 97 da 84 5a d5 d6 4f 8e 0 10 66 00 00 00 01 00 00 20 00 00 00 77 dd c7 86 d 19 23 a7 66 ad 29 5d 67 97 87 2f 00 00 00 00 0e b 62 1: c2 d2 95 3f 32 bc 04 a6 0e c7 d1 0b 4d 1b a 0b 5c d1 0a 0a 68 a9 ec 71 2e fe 72 60 40 000 b 03 b6 67 ae 37 80 7c fe 64 50 7 de 00 4f c7 d6 c ed 9 c72 a5 2b 61 81 40 74 e3 2c 66 a1 89 bf		
Report Text	Hex min Decode Mout Q 100% ▼ Pro Login Data https://twitter.com/ twitter.com/ https://twitter.com/sessi session[username_or_et peterwilson.win7@live.co session[password] 01 00 00 00 d0 8c 9d df 01 16 e5 2789 3d ae 63 00 00 eb e3 55 1d b8 b8 ef 66 co 80 00 00 00 20 00 00 20 00 7d 95 41 9a 3b 67 41 9a 61 00 55 31 5a 74 3a 1b ca 73 22 60 b1 13 95 d8 4f e6 e https://twitter.com/ 1	Doc Transcrip evious Item Next ions mail] com 15 dl 11 8c 7a 00 dd 4 00 00 02 00 00 00 00 159 0e fc 92 0L b7 df 0 00 00 fa 7f ad 5f ff 00 00 00 fa 7f ad 5f ff 00 08 10 00 00 01 6f 07 3 d6 83 ff 65 19 ae ac 2 62 9f 10 60 ff 03 23 6 d	fr (2 97 eb 01 00 00 00 d6 97 da 84 5a d5 d6 4f 8e 0 10 66 00 00 00 01 00 00 20 00 00 00 77 dd (7 86 d 19 25 a7 66 ad 29 5d 67 97 87 2f 00 00 00 00 0e b 62 12 (2 d2 95 3f 32 bc 04 a6 0e (7 d1 0b 4d 1b ba 0b 5c d1 0a 0a 88 a9 e7.12 ef e7 26 04 00 00 00 b 20 b5 c4 0a a 37 80 7c fc e6 45 07 de 00 4f c7 d6 ex 49 c72 a5 2b 61 81 40 74 e3 2c 66 a1 89 bf		
Com In Text	Hex min Decode Mout Q 100% ▼ Pro Login Data https://twitter.com/ twitter.com/ https://twitter.com/sessi session[username_or_ei peterwilson.win7@live.c session[password] 01 00 00 00 08 c9d dr 01 16 e5 2789 3d ae 63 00 00 eb e3 55 1d b6 b8 ef dc cd 80 00 00 00 02 00 00 20 00 cd 05 31 5a 74 3a 1b ca 73 22 60 b1 13 95 cd 84 fe 6e https://twitter.com/ 1	Doc Transcrip evious Item Next ions mail] com 15 dl 11 8c7a 00 d0 4 00 00 02 00 00 00 00 159 0e fc92 01 b7 d1 0 00 00 fa 77 ad 5f 6f 00 0.081 00 00 00 16 07 0 d6 83 f6 65 19 ae ac 2 62 9f 10 60 f0 03 23 6c	f (2 97 eb 01.00 00 00 d6 97 da 84 5a d5 d6 4f 8e 10 66 00 00 00 01 00 00 20 00 00 00 77 dd (7 86 d 19 23 a7 66 ad 29 5d 67 97 87 2f 00 00 00 00 0e b 65 1/2 cd 29 53 f 52 bc 04 a6 0e c7 d1 0b 4d 1b 3 0b 5c d1 00 a 08 89 9e 71 2e f 72 50 40 00 00 00 2 01 0 a6 37 80 7c f ce 6 45 07 de 00 4f c7 d6 2 d9 c72 a5 2b 61 81 40 74 e3 2c 66 a1 89 bf		
Report Text	Image: Hex Image: Decode Image: Mexicology Image: Decode Image: Decode Image: Decode Image: Deco	Doc Transcrip evious Item Next lons mail] 500 15 dl 11 8c 7a 00 d0 4 00 00 02 00 00 00 00 159 0e fc 92 01 b7 d1 00 00 fa 77 ad 57 fof 00 108 10 00 00 16 73 66 19 fe 55 19 ae ac2 62 9f 10 60 f0 03 23 6c	f (2 97 eb 01.00 00 00 d6 97 da 84 5a d5 d6 4f 8e 01 06 00 00 01 00 00 00 00 00 00 07 dd c7 86 d 19 23 a7 66 ad 29 5d 67 97 87 2f 00 00 00 00 0e b 62 1, c2 d2 95 3f 32 bc 04 a6 0e c7 d1 0b 4d 1b 9a 0b 5c d1 0a 0a 08 a9 ec 71 2e fe 72 60 40 00 00 c4 b3 b7 7a e 37 80 7c fc e6 45 07 de 00 4f c7 d6 : ed 9c 72 a5 2b 61 81 40 74 e3 2c 66 a1 89 bf		
Report Text	Hex Imin Decode Imin Dut 100% ▼ Protect Login Data https://twitter.com/ https://twitter.com/ session[username_or_et peterwilson.win7@live.c session[password] 01 00 00 00 d8 8:9d dr01 16 65 2769 3d ac 63 00 00 bb bb 8 ef of cod 80 00 00 00 20 00 20 00 749 34 19 3b 67 41 9a 61 00 55 31 5a 74 3a 16 ca 73 22 60 b1 13 95 d8 4f e6 ehttps://twitter.com/ 1 0d/21/13 03:47:43PM 0	Doc Transcrip evious Item Next lons mail] form 15 dl 11 8c 7a 00 d0 4 00 00 02 00 00 00 00 159 0e fc92 01 b7 d0 00 00 fa 7f ad 5f 6f 00 00 00 fa 7f ad 5f 6f 00 00 00 fa 65 19 ae ac 2 62 9f 10 60 f0 03 23 6c	fr (2 97 eb 01.00 00 00 d6 97 da 84 5a d5 d6 4f 8e 10 10 66 00 00 01 00 00 00 06 97 da 84 5a d5 d6 4f 8e 10 10 66 00 00 01 00 00 20 00 00 00 77 dd c7 86 d 19 23 a7 66 ad 29 5d 67 97 87 2f 00 00 00 00 0e b6 21 c2 d2 95 3f 32 bc 04 a6 0e c7 d1 0b 4d 1b 93 0b 5c d1 0a 0a 08 a9 ec 7 12 ef 72 60 40 00 00 12 d0 3b 67 as 37 80 7c fr ce 64 50 7 de 00 4f c7 d6 : ed 9c 72 a5 2b 61 81 40 74 e3 2c 66 a1 89 bf		
Report Text	Hex min Decode Pre m Out <a>100% Pre Login Data https://twitter.com/ https://twitter.com/sessisession[username_or_etre https://twitter.com/sessisession[username_or_etre peterwilson.win7@live.c session[password] 01 00 000 od 8c 9d dr 01 16 e5 2f 89 3d ae 63 00 00 eb ef 65 cd 00 00 00 00 00 00 00 00 00 20 00 20 00 7 49 54 19 3b 67 41 9a 61 00 55 31 5a 74 3a 1b ca 73 22 60 bil 13 95 d8 4f e6 e https://twitter.com/ 1 1 04/21/13 03:47:43PM 0	Doc Transcrip evious Item Next lons mail] com 15 dl 11 8c 7a 00 d0 4 00 00 02 00 00 00 00 00 159 0e fc 92 0l b7 d7 00 00 fc 74 d3 76 f0 00 00 00 fa 74 d3 76 f0 00 00 00 fa 74 d3 76 f0 00 00 00 fa 74 d3 76 f0 03 0 00 fa 63 f6 65 19 ae ac 2 62 9f 10 60 f0 03 23 60	picture Fields Item Item		
Report Text	Hex min Decode m Out 0 100% ▼ Protect Login Data https://twitter.com/ twitter.com/ https://twitter.com/sessis session[username_or_eti peterwilson.win7@live.co session[password] 01.00 00 00 d0 8c 9d df 01 16 e5 2f 89 3d ae 63 00 00 eb ef of sc 00 00 00 00 20 00 00 7d 95 41 9a 3b 67 41 9a 61 00 55 31 5a 74 3a 1b ca 73 22 60 b1 13 95 d8 84 fe 6e https://twitter.com/ 1 1 0 0 Chrome (Windows)	Doc Transcrip evious Item Next ions mail] com 15 dl 11 8c 7a 00 d0 4 00 00 02 00 00 00 00 00 159 0c fc 92 0l b7 d0 00 00 fa 7f ad 5f 6f 00 00 00 fa 5f 6 f5 19 ae ac 2 62 9f 10 60 f0 03 23 6c	bit Picture () Fields Item Item		

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:

ive Search Results
B-Live Search {"facebook", "twitter"} (ID:1000) performed 06/06/2013 14:38:28 16238 hit(s) in 856 file(
= Text Query: "facebook" <ansi, case="" insensitive=""> 8283 hit(s) in 520 file(s)</ansi,>
#-Allocated Space 5686 hit(s) in 390 file(s)
In Unallocated Space 2597 hit(s) in 130 file(s)
é- Text Query: "twitter" <ansi, case="" insensitive=""> 7955 hit(s) in 336 file(s)</ansi,>
Allocated Space 5162 hit(s) in 202 file(s)
Inallocated Space 2793 hit(s) in 134 file(s)

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
\star	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
\star	1	RIT Sports Info	@RIT sports	05/02/2013 02:12:38 AM	BB <a data-q<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 7.vmdk · Partition 1</th><th>File offset 120863226</th>	Windows 7.vmdk · Partition 1	File offset 120863226
*	3	RIT Sports Info	@RIT sports	05/04/2013 05:52:21 PM	<a class="</th" href="//search?q=%23LLWTennisChampionship&</th><th>Windows 7. vmdk - Partition 1</th><th>Physical Sector 2923740</th></tr><tr><th>*</th><th>5</th><th>RIT NEWS</th><th>@RITNEWS</th><th>05/04/2013 05:19:39 PM</th><th>Coverage of <th>Windows 7. vmdk • Partition 1</th><th>Physical Sector 2923794</th>	Windows 7. vmdk • Partition 1	Physical Sector 2923794
*	10	RIT Sports Info	@RIT sports	05/04/2013 04:21:47 PM	<a class="</th" href="//search?q=%23LLWTennisChampionship&</th><th>Windows 7. vmdk · Partition 1</th><th>Physical Sector 2923838</th></tr><tr><th>*</th><th>11</th><th>RIT Sports Info</th><th>@RIT sports</th><th>05/04/2013 04:16:25 PM</th><th>BB <th>Windows 7.vmdk · Partition 1</th><th>Physical Sector 2923851</th>	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	@RIT sports	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	@RIT sports	05/04/2013 07:17:30 PM	<a class="twitt</th><th>Windows 7. vmdk · Partition 1</th><th>Physical Sector 30401977</th></tr><tr><th>*</th><th>17</th><th>RIT Sports Info</th><th>@RIT sports</th><th>05/04/2013 06:57:06 PM</th><th><a href=" href="//search?q=%23RIT&src=hash" search?q="%23LLWTennisChampionship&</th"><th>Windows 7. vmdk · Partition 1</th><th>Physical Sector 30401989</th>	Windows 7. vmdk · Partition 1	Physical Sector 30401989
*	18	RIT Sports Info	@RIT sports	05/04/2013 06:54:48 PM	<a data-query<="" href="//search?q=%23LLWTennisChampionship&</th><th>Windows 7. vmdk · Partition 1</th><th>Physical Sector 30402001</th></tr><tr><th>*</th><th>19</th><th>RIT NEWS</th><th>@RITNEWS</th><th>04/23/2013 06:30:15 PM</th><th><th>Windows 7. vmdk · Partition 1</th><th>Physical Sector 31080725</th>	Windows 7. vmdk · Partition 1	Physical Sector 31080725
*	21	RIT Sports Info	@RIT sports	04/25/2013 10:41:21 PM	BB <a data-q<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 7. vmdk • Partition 1</th><th>Physical Sector 50094657</th>	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	@RIT sports	04/21/2013 07:17:54 PM	<a data-query<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 7. vmdk • Partition 1</th><th>Physical Sector 50280062</th>	Windows 7. vmdk • Partition 1	Physical Sector 50280062
*	24	RIT Sports Info	@RIT sports	04/21/2013 07:17:54 PM	<a data-query<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 7. vmdk · Partition 1</th><th>Physical Sector 16155230</th>	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
\star		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/288029904611462/9	Looking at Facebook group with group id: 288029904611462	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 activity. 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).





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:



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 <u>peterwilson.win7@gmail.com</u>, 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:

End State € End State € End Profes End Profes End Profes End Profes State (237) (27) End Profes End Profes End Profess End Profes End Profess End Profess End Profess <t< th=""><th>Name 0029482-00000012.eni 0029482-00000015.eni 0029482-00000016.eni 029182-00000016.eni 0873738-0000006.eni 0571952-0000006.eni 0517952-00000016.eni 0517952-00000016.eni 1972755-00000016.eni 1972755-00000016.eni 1972755-0000016.eni 1972755-0000016.eni 19747026-0000016.eni</th><th></th><th>Instal Deploy Time Zine: East Select Op(4)2012 Sinal with Attachment Op(4)2012 Sinal with Attachment Op(4)2012 Sinal with Attachment Op(6)2012 Sinal with Attachment Op(6)2012 Sinal with Text and Ptuebook account Op(6)2012 Sinal with Text and the week Peter Week Comforts you as finding on textbook</th><th>ern standard inne (trem koal inderne) To "Vindeuw" Gaalf - detervition, Win7Bgesal.com>, Windeusd Gaalf - Ø Vindeuws Gaalf - detervition, Win7Bgesal.com>, Wandeued Gaalf - M "Vindeuws Gaalf - detervition, Win7Bgesal.com>, Tearevition, Vindeuws Generition, Win7Bgesal.com>, Tearevition, Windeuws Generition, Win7Bgesal.com>, Tearevition, Windeuws Generition, Win7Bgesal.com>, Windeuws Generition, Windeuws Generition,</th><th>Tion Tive Account* «PeterWison.Win7@ive.com> Peter Wison cytemison.win8@ive.com> Tive Account* «PeterWison.Win7@ive.com> Peter Wison cytemison.win8@ive.com> PeterWison cytemison.win8@ive.com> Peter Wison cytemison.win8@ive.com> PeterWison cytemison.win8@ive.com> Peter Wison cytemison.win8@ive.com> PeterWison cytemison.win8@ive.com> Peter Wison cytemison.win8@ive.com> PeterWison cytemison.win8@ive.com></th></t<>	Name 0029482-00000012.eni 0029482-00000015.eni 0029482-00000016.eni 029182-00000016.eni 0873738-0000006.eni 0571952-0000006.eni 0517952-00000016.eni 0517952-00000016.eni 1972755-00000016.eni 1972755-00000016.eni 1972755-0000016.eni 1972755-0000016.eni 19747026-0000016.eni		Instal Deploy Time Zine: East Select Op(4)2012 Sinal with Attachment Op(4)2012 Sinal with Attachment Op(4)2012 Sinal with Attachment Op(6)2012 Sinal with Attachment Op(6)2012 Sinal with Text and Ptuebook account Op(6)2012 Sinal with Text and the week Peter Week Comforts you as finding on textbook	ern standard inne (trem koal inderne) To "Vindeuw" Gaalf - detervition, Win7Bgesal.com>, Windeusd Gaalf - Ø Vindeuws Gaalf - detervition, Win7Bgesal.com>, Wandeued Gaalf - M "Vindeuws Gaalf - detervition, Win7Bgesal.com>, Tearevition, Vindeuws Generition, Win7Bgesal.com>, Tearevition, Windeuws Generition, Win7Bgesal.com>, Tearevition, Windeuws Generition, Win7Bgesal.com>, Windeuws Generition, Windeuws Generition,	Tion Tive Account* «PeterWison.Win7@ive.com> Peter Wison cytemison.win8@ive.com> Tive Account* «PeterWison.Win7@ive.com> Peter Wison cytemison.win8@ive.com> PeterWison cytemison.win8@ive.com>
E Indi Achess E Indi E Indi E Indi Achess E Indi E Indi Achess E Indi E Indi Achess E Indi E Indi E Indi Achess E Indi E	Name 00294825-0000012.emi 00294825-0000018.emi 00294825-0000018.emi 00294825-0000018.emi 0291747-0000018.emi 0875738-0000016.emi 0875738-0000016.emi 02167455-00000016.emi 0217495-00000016.emi 0217495-00000016.emi 18177995-0000016.emi 18177995-0000018.emi 18177995-00000018.emi	Submit Time 4(24)2013 9:14:02 PM 4(24)2013 9:13:03 PM 5(3)2013 9:5:29 PM (5(3)2013 15:32:8 PM (5(1)2013 11:41:88 PM (4(1)2013 11:41:88 PM (4(1)2013 11:601 AM 3(7)2013 11:19:33 PM (5(1)2013 11:19:33 PM (Subject (04/24/2013 Enail with Attachment 04/24/2013 Enail with Attachment 05/02/2013 Enail with Attachment 05/02/2013 Caly Enail with Text and Poture Attachments 05/02/2013 Caly Enail with Text and Poture Attachments 05/02/2013 Caly Enail with Text and Poture Attachments 05/02/2013 Caly Enail with a cale of the week. Poter Without Conference Que as a finder of Facebook	To "Window? Gaal" Overwiken. Win?Bgraal.com., Windowel Gaal" O Window? Gaal" Overwiken. Win?Bgraal.com., Window? Monto-Steven. "Window? Gaal" Overwiken. Win?Bgraal.com., Window? Gaal" O Window?Seen Forenics Overwiken. Win?Bgraal.com., Overwiken "PaterWiken. WinBgraal.com" Overwiken. WinBgraal.com, Window? Modow?Seen Forenics Overwiken. WinBgraal.com, Window?	From "Ive Account" deternilison.win7@live.com> Peter Wilson deternilison.win7@live.com> Tue Account" deternilison.win7@live.com> Peter Wilson deternilison.win7@live.com> Peter Wilson deternilison.win7@live.com> Teactbook" domitison-win7@live.com>
End by bits = Soluti C3 (27) (27) = Soluti C3 (27) (27) (27) = Soluti C3 (27) (27) (27) = Soluti C3 (27) (27) (27) (27) = Soluti C3 (27) (27) (27) (27) (27) (27) (27) (27)	0029482-0000012.emi 0029482-0000013.emi 0029482-000001E.emi 0029482-0000001E.emi 0029482-0000001E.emi 00291982-00000001E.emi 00219195-00000004.emi 00219195-00000012.emi 19827855-00000019.emi 19127955-00000019.emi	4/24/2013 9:14:02 PM 4/24/2013 9:31:30 PM 5/3/2013 4:35:29 PM (5/3/2013 1:35:03:28 PM (5/1/2013 1:14:38 PM (4/13/2013 1:58:01 PM (3/7/2013 1:15:01 PM (5/1/2013 1:15:94 PM (5/12/013 1:15:94 PM (04(24/2013) Einal with Attachment 04(24/2013) Einal with Attachment 04(24/2013) Einal with Einal 05(20)(2013) Calve, Einal 05(20)(2013) Calve, Einal with Text and Picture Attachments 09(12/2013) Calve, Einal with Text and Picture Attachments 09(12/2013) Calve, Einal with Calve, Cal	"Vindows Gradi" Ceterrilison. Win7Bghal.com>, Windows Gradi" Ceterrilison. Win7Bghal.com>, WindowsSeren Windows Gradi "deterrilison. Win7Bghal.com>, WindowsSeren WindowsSeren Forensis Ceterrilison. Win7Bghal.com>, "Heatwildon "Peterwildon.Win8Bghal.com", "deterrilisonWindowsSeren Forensis ceterrilison "Peterwildon.Win8Bghal.com", "deterrilisonWindowsSeren Forensis ceterrilison	Tuke Account" «PeterWilson.Win7@like.com> PeterWilson opeterwilson.win8@like.com> Tuke Account"> OeterWilson.Win7@like.com> PeterWilson opeterwilson.win8@like.com> PeterWilson opeterwilson.win8@like.com>
Definition (27) (27) Definition (27) Definion (27) De	00294823-0000013.eml 00294823-000001E.eml 00294823-0000001E.eml 05713925-00000010.eml 05713925-00000009.eml 05127455-0000009.eml 05127455-00000019.eml 16127795-00000015.eml	4(24)2013 9:31:30 PM 5(3)2013 9:35:29 PM (5(3)2013 5:03:28 PM (5(1)2013 11:41:58 AM 3(7)2013 11:41:58 AM 4(13)2013 11:58:01 AM 3(7)2013 11:19:43 AM 5(1)2013 11:19:43 AM 4(14)2013 11:19:43 AM	04(24(20)3) Email with Attachment 05(81)(20)3) Doly Email 05(81)(20)3) Doly Em	WindowsSeven Forensics https://www.com , WindowsSeven Windows? Gmail https://www.com , WindowsSeven Forensics https://www.com , https://www.com"/>https://www.com, <a <peterwilson.win7@live.com="" href="https://www.c</td><td>Peter Wilson <pre>cpeterwilson.win8@live.com> Ture Acount"> Peter Wilson <pre>cpeterwilson.win8@live.com> Peter Wilson <pre>cpeterwilson.win8@live.com> "Bacebook" com> "Bacebook" com> "Bacebook" com> "Bacebook" com> </pre></pre>	
Implement (127 / 127) Implement (127 / 127) Implement (127 / 127) Implement (127 / 127) <tr< td=""><td>00294823-000001E.emi 00294823-000001F.emi 0291274*000001D.emi 05713925-0000000.emi 021F1455-0000000F.emi 021C715*0000001C.emi 13F27855-0000019.emi 161D7799-0000016.emi</td><td>5(3)2013 4:35:29 PM (5(3)2013 5:03:28 PM (5)1/2013 11:41:58 AM 3)7/2013 11:41:58 PM (4)13/2013 11:43:8PM (5)1/2013 11:19:43 AM 5)1/2013 11:19:43 AM</td><td>05(03)2013 Daty Email; 05(03)2013 Daty Email 05(03)2013 Daty Email with Text and Picture Attachments 05(01)2013 Daty Email with Text and Picture Attachments 055778@mail.nt.edu added to your Facebook account Top 3 poets for you on Google+ this weak. Pater Wison confined you as a fined on Facebook</td><td>"Windows? Gmail" <peterwison.win7@gmail.com>, Windows8 Gmail" & WindowsSeven Forensics <peterwison.win7@gmail.com>, "PeterWison.Win8@gmail.com>, "PeterWison.Win8@gmail.com" <pre>>////@gmail.com></pre></peterwison.win7@gmail.com></peterwison.win7@gmail.com></td><td>"Live Account" <peterwilson.win7@live.com> Peter Wilson <peterwilson.win8@live.com> Peter Wilson <peterwilson.win8@live.com> "Pacebook" <notfication+kr4yyblynkma@facebookmail.o< td=""></notfication+kr4yyblynkma@facebookmail.o<></peterwilson.win8@live.com></peterwilson.win8@live.com></peterwilson.win7@live.com></td></tr<>	00294823-000001E.emi 00294823-000001F.emi 0291274*000001D.emi 05713925-0000000.emi 021F1455-0000000F.emi 021C715*0000001C.emi 13F27855-0000019.emi 161D7799-0000016.emi	5(3)2013 4:35:29 PM (5(3)2013 5:03:28 PM (5)1/2013 11:41:58 AM 3)7/2013 11:41:58 PM (4)13/2013 11:43:8PM (5)1/2013 11:19:43 AM 5)1/2013 11:19:43 AM	05(03)2013 Daty Email; 05(03)2013 Daty Email 05(03)2013 Daty Email with Text and Picture Attachments 05(01)2013 Daty Email with Text and Picture Attachments 055778@mail.nt.edu added to your Facebook account Top 3 poets for you on Google+ this weak. Pater Wison confined you as a fined on Facebook	"Windows? Gmail" <peterwison.win7@gmail.com>, Windows8 Gmail" & WindowsSeven Forensics <peterwison.win7@gmail.com>, "PeterWison.Win8@gmail.com>, "PeterWison.Win8@gmail.com" <pre>>////@gmail.com></pre></peterwison.win7@gmail.com></peterwison.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com> Peter Wilson <peterwilson.win8@live.com> Peter Wilson <peterwilson.win8@live.com> "Pacebook" <notfication+kr4yyblynkma@facebookmail.o< td=""></notfication+kr4yyblynkma@facebookmail.o<></peterwilson.win8@live.com></peterwilson.win8@live.com></peterwilson.win7@live.com>
B (13) (127) (127) B (13) (127) (127) B (13) Addresses	00294823-000001F.emi 0290174F-000001D.emi 05713925-0000000.emi 083F2738-0000000F.emi 0E1C7415-0000001C.emi 13F27355-0000019.emi 161D7F99-0000019.emi 1814002C-0000020.emi	5/3/2013 5:03:28 PM (5/1/2013 11:41:58 AM 3/7/2013 1:141:58 PM (4/13/2013 1:58:01 AM 3/7/2013 1:58:01 AM 5/1/2013 11:19:43 AM 4/05/2013 11:329 PM (05/03/2013 Daily Email 05/01/2013 Daily Email with Text and Picture Attachments ply657988mal.rit.edu added to your Facebook account Top 3 posts for you on Google+ this week Peter Wilson confirmed you as a friend on Facebook	WindowsSeven Forensics <peterwilson.win7@live.com>, "PeterWilson "PeterWilson.Win8@gmail.com" <peterwilson.win8@gmail.com>, Windo WindowsSeven Forensics <pre>cpeterwilson.win7@gmail.com></pre></peterwilson.win8@gmail.com></peterwilson.win7@live.com>	Peter Wilson <peterwilson.win8@live.com> Peter Wilson <peterwilson.win8@live.com> "Facebook" <notfication+kr4yybkynkma@facebookmal.o< td=""></notfication+kr4yybkynkma@facebookmal.o<></peterwilson.win8@live.com></peterwilson.win8@live.com>
il and Address	029D174F-0000001D.eml 05713925-0000000A.eml 0B3F2F38-0000000F.eml 0E1CF1456-0000009.eml 0E1C7415-0000001.eml 13F27855-00000019.eml 161D7799-00000016.eml	5/1/2013 11:41:58 AM 3/7/2013 11:41:58 AM 4/13/2013 1:58:01 AM 3/7/2013 1:58:01 AM 5/1/2013 11:19:43 AM 4/06/2013 11:39:31 A	05/01/2013 Dafy Email with Text and Picture Attachments piv6579@mail.nit.edu added to your Facebook account Top 3 posts for you on Google+ this week Pater Wison confirmed you as a friend on Facebook	"PeterWison.Win8@gmail.com" <peterwison.win8@gmail.com>, Windo WindowsSeven Forensics <peterwison.win7@gmail.com></peterwison.win7@gmail.com></peterwison.win8@gmail.com>	Peter Wilson <peterwilson.win8@live.com> "Facebook" <notification+kr4yybkynkma@facebookmail.co< td=""></notification+kr4yybkynkma@facebookmail.co<></peterwilson.win8@live.com>
Constant (241 (241)) Constant (241 (05713925-000000A.emi 083F2F38-000000F.emi 0C1F1456-0000009.emi 0E1C7415-0000001C.emi 13F27855-00000019.emi 16107F99-0000016.emi 1874002C-00000020.emi	3/7/2013 1:14:38 PM (4/13/2013 1:58:01 AM 3/7/2013 1:13:29 PM (5/1/2013 1:19:43 AM 4/56/2013 11:29:21 A	pix6578@mail.rit.edu added to your Facebook account Top 3 posts for you on Google+ this week Peter Wilson confirmed you as a friend on Facebook	WindowsSeven Forensics <pre>cpterwilson.win7@gmail.com></pre>	"Facebook" <notification+kr4yybkynkma@facebookmail.o< td=""></notification+kr4yybkynkma@facebookmail.o<>
	083F2F3B-000000F.eml 0C1F1456-0000009.eml 0E1C7415-000001C.eml 13F27855-0000019.eml 161D7F99-0000016.eml 1874002C-0000020.eml	4/13/2013 1:58:01 AM 3/7/2013 1:13:29 PM (5/1/2013 11:19:43 AM 4/36/2013 11:29:21 A	Top 3 posts for you on Google+ this week Peter Wilson confirmed you as a friend on Facebook	a describer of 20 and and	
Construction (155 (155)) Construction (155 (155)) Construction (157 (155)) Constructi	0C1F1456-0000009.eml 0E1C7415-0000001C.eml 13F27855-0000019.eml 161D7F99-00000016.eml 18740D2C-0000020.eml	3/7/2013 1:13:29 PM (5/1/2013 11:19:43 AM 4/36/2013 11:32:21 A	Peter Wilson confirmed you as a friend on Facebook	Deterwision.win/wamai.com	"Google+ team" <noreply-475ba29f@plus.google.com></noreply-475ba29f@plus.google.com>
Bind Control [2/2] Bind Adverse [15/13] Bind [15/13] Bind [15/13] Bind Adverse [15/13] Bind Adverse [15/13] Bind [15/13]	0E1C7415-0000001C.eml 13F27855-00000019.eml 161D7F99-00000016.eml 1874002C-00000020.eml	5/1/2013 11:19:43 AM		WindowsSeven Forensics <pre>cpeterwilson.win7@gmail.com></pre>	"Facebook" <notification+kr4v bk="" mkma@facebookmail.<="" td=""></notification+kr4v>
B → Dispire Mane (13/137) C Dispire Mane (13/137) Dispire Mane	13F27855-00000019.eml 161D7F99-00000016.eml 1B740D2C-00000020.eml	4/26/2013 11-32-21 A	05/01/2013 Daily Email with Text and Picture Attachments	"Windows7 Gmail" «PeterWilson, Win7(Bomail.com>, "Windows8 Gmail" «P	"Live Account" «PeterWilson Win7@live.com>
E = Brail Adverses (157 157) E = Brail Adverses (161D7F99-00000016.eml 1B740D2C-00000020.eml	and the second state of th	04/26/2013 Dath Email	"Windows7 Gmail" «Peterillikon Win7@mail.com>. "Windows8 Gmail" «P	"Live Account" «PeterWilson Win7@live.com»
patentisma netility and cons (24) (20) patentisma netility and (27) (27) patentisma netility and (1874002C-00000020.eml	4/25/2013 10-15-45 P	04/25/2013 Date Email	Pater Wilson contension win8/Tilva com>, Window/Savan Forencics cR	neterulion win3@omail.com
potensica webged.com (10, 10) p	107 100-20 00000000000000000000000000000000	5(4(2013 3:47:16 PM (05/04/2013 Daly Email	Peter Wilson (peterwison win@filve.com), WindowsSeven Forencics (P	peterwison win8@gmail.com
a potentica webgina.com (+) (+) a potentica webgina.com	18692825-00000010 aml	4/21/2013 3-53-37 DM	04/21/2013 Date Email	"Windows? Gnail" (Detertilizen Win?Romail.com), "Windows? Gnail" (R	Time Account" «Paterialicon Win7/Bitue com»
	25840803-00000014 aml	4/25/2013 10-07-32 P	Da: 04/25/2013 Daly Email	"Gnal Account" creteriolicity with by gran. Contry, with both of and in Contry	"Two Account" «Paterializon Min76ive com>
Contemports(11) Contemports(11) Contemports(11) Contemports(12) Contemports(12) Contemports(12)	29900141-00000000 cml	2/20/2012 10:07:22 4	Ton 2 ports for you on Condet, this week	netawilcon win78amal.com	"Coordina team" crossedu 475ha2058ebur acoola com>
Bit End Domars [2/2] Bit End (244 / 244)	20090111-00000000.8ml	4/20/2010 10:07:00 Mill	04/10/2013 Date Earl	Madeus Fauer Fauer de Antoi Mar Mar Mar al anno - Madeus Fau	about the minimum and the second second
Bind Software (135 / 135) Bind Software (135 / 135) Bind Addresses (135 / 135) Email (244 / 244)	3556/F32/0000015/6m	4/35/2013 10/30/31 0	Day 04/26/2013 Daily Email	WindowsSeven Porensiss Crece wison, win2 ggilal.com2, windowsSev	peterwisen.windpgmail.com
E ⊂ Emai Addresses (135/135) Emai (244/244)	36046268-00000017.emi	4/25/2013 10:30:21 P	Ret 04/25/2013 Daily Email	WindowsSeven Porensics <pre>cpecerwisson.win/ggmail.com> WindowsSeven Porensics <pre>cpecerwisson.win/ggmail.com></pre></pre>	peterwison.winoggmail.com
Emal (244/244)	SELC217A-0000001A.em	4/26/2013 11:51:59 A	04)26)2013 Daily Elital	windowso anal creter wison, windgginal, com2, recer wison creter w	Peter wison specerwison windgelver.com
	466/3ESA-0000018.em	4/26/2013 1:55:34 AM	Top 3 posts for you on Googe+ this week.	peterwison.win/upgmail.com	Google+ team <norepiy-4 pius.google.com="" sba29rg=""></norepiy-4>
	494C12/8-0000001.em	3///2013 12:32:57 PM	Get Gmail on your mobile phone	Peter Wilson <peterwilson.wn @gmail.com=""></peterwilson.wn>	Gmail Team <mail-noreply algoogle.com=""></mail-noreply>
	4908639F-0000000B.eml	3/7/2013 1:22:08 PM (Test	peterwilson.win7@gmail.com	Peter Wilson <p(w5578@rit.edu></p(w5578@rit.edu>
	4A486650-00000015.em	4/25/2013 10:08:24 P	Fw: 04/25/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
	4EC70636-00000005.eml	3/7/2013 12:50:01 PM	Just one more step to get started on Facebook	peterwilson.win7@gmail.com	"Facebook" <confirm+acgv02xj3awxzb24ud2lun0bnbw< td=""></confirm+acgv02xj3awxzb24ud2lun0bnbw<>
	54EE6884-00000011.emi	4/23/2013 10:46:42 P	04/23/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com>, WindowsSeven Forensics <p< td=""><td>peterwilson.win8@gmail.com</td></p<></peterwilson.win8@live.com>	peterwilson.win8@gmail.com
	61AS00CE-00000006.eml	3/7/2013 12:50:01 PM	Welcome to Facebook - get started now!	WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Facebook" <update+kr4yybkynkma@facebookmail.com:< td=""></update+kr4yybkynkma@facebookmail.com:<>
	6D732103-00000003.eml	3/7/2013 12:32:57 PM	Customize Gmail with colors and themes	Peter Wilson <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	Gmail Team <mail-noreply@google.com></mail-noreply@google.com>
	6DFA3582-00000002.eml	3/7/2013 12:32:57 PM	Import your contacts and old email	Peter Wilson <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	Gmail Team <mail-noreply@google.com></mail-noreply@google.com>
	73841F54-00000007.emi	3/7/2013 12:57:11 PM	peterwilson.win7@live.com added to your Facebook account	WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Facebook" <notification+kr4yybkynkma@facebookmail.c< td=""></notification+kr4yybkynkma@facebookmail.c<>
	762F4607-00000004.eml	3/7/2013 12:35:05 PM	Getting started on Google+	peterwilson.win7@gmail.com	"Google+ team" <noreply-daa26fef@plus.google.com></noreply-daa26fef@plus.google.com>
	77585766-00000008.eml	3/7/2013 12:58:13 PM	WindowsEight Forensics confirmed you as a friend on Facebook	WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Facebook" <notification+kr4yybkynkma@facebookmail.o< td=""></notification+kr4yybkynkma@facebookmail.o<>
	7F4D558C-0000000C.eml	3/16/2013 3:01:03 AM	Top 3 posts for you on Google+ this week	peterwilson.win7@gmail.com	"Google+ team" <noreply-475ba29f@plus.google.com></noreply-475ba29f@plus.google.com>
	00294823-00000016.eml	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email	"Gmail Account" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
	10A94C72-00000004.eml	3/7/2013 12:35:05 PM	Getting started on Google+	peterwilson.win7@gmail.com	"Google+ team" <noreply-daa26fef@plus.google.com></noreply-daa26fef@plus.google.com>
	10E66C58-00000019.eml	4/25/2013 10:30:21 P	Re: 04/25/2013 Daily Email	WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	peterwilson.win8@gmail.com
	1238360D-0000001B.eml	4/26/2013 11:32:21 A	04/26/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
	16883D48-00000010.eml	4/21/2013 3:53:37 PM	04/21/2013 Daily Email	"Windows7 Gmail" <peterwilson, win7@gmail.com="">, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td></p<></peterwilson,>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
n -	188E6784-00000013.emi	4/24/2013 9:14:02 PM	04/24/2013 Email with Attachment	"Windows7 Gmail" «PeterWilson, Win7@mmail.com>, "Windows8 Gmail" «P	"Live Account" <peterwilson bive.com="" win7=""></peterwilson>
	188E6784-00000014 emi	4/24/2013 9-31-30 PM	04/24/2013 Enail with Attachment	WindowsSeven Ecrensics (PeterWilson Win78ilve com), WindowsSeven	Peter Wilson (neterwison win8@live.com)
	188E6784-00000026.eml	5/3/2013 4:35:29 PM (05(03)2013 Daily Final:	"Windows7 Gmail" (Peterillikon Win7@mail.com), "Windows8 Gmail" (P	"Tive Account" «PeterWilson Win7@live.com»
	18856784-00000020.cm	5/3/2013 5:03:28 PM (05/03/2013 Daly Enal	Windows Seven Errenzing «Detertilition Win76live com», "Detertilition	Pater Wilcon cnaterwilcon win8@live com>
	230064FE-00000017 and	4/25/2013 10:08:24 P	Fur 04/25/2013 Daily Email	"Vindows7.Gmail" (Reterialison Win78hmail.com)	"Tive Account" «Deteriation Win7/Rive com>
	24562070 00000007.8ml	2/16/2010 10:00:24 P	Two Organization of Canada Likkin unad	windows/ datasi scoto mison, win/@glidi.com/	"Country Loop" controls (2010) (2010)
	27562570-0000000C.EMI	a)10/2013 3:01:03 AM	Top 3 posts for you on gauger this week	poterwoor.wei/opginal.com	Google Libert Commence (Compared Compared Compar
	21034002-00000000.em	3/25/2013 10:07:33 A	Cat Card as you with a base	petermoutumin geginal.com	Good Team and excel decede and
	2ME10232-0000001.0ml	3//2013 12:32:5/ PM	declariar on your mode prone	Peter wiscill specerwiscill with openalized by the second openalized by	sinar ream smarriorepry@0000e.com>
	285970H6-00000021.eml	5/1/2013 11:19:43 AM	Usiui J2013 Uairy Email with Text and Picture Attachments	windows/ umail <pre>reterwision.win/@gmail.com>, "Windows8 Gmail" <p< pre=""></p<></pre>	LINE INCOURT CHARACTERING AND ZOURAR COM-

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

In the case of email sent to <u>peterwilson.win7@live.com</u>, 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:
Email Rens 4 b	· 문 문	8 / 1		🗑 💼 🔟 Email 🔹 Display Time Zone: Eas	stern Standard Time (From local machine)		8 0
er and Status Email Archives		Name	Submit Time	Subject	То	From	
Email by Date		00294823-00000013.emi	4/24/2013 9:31:30 PM	04/24/2013 Email with Attachment	WindowsSeven Forensics <peterwilson.win7@live.com>, WindowsSeven</peterwilson.win7@live.com>	Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com>	
er == Submitted (237/237) = = Delivered (127/127)		0290174F-0000001F.emi	5/3/2013 5:03:28 PM (5/1/2013 11:41:58 AM	Usju3/2013 Daily Email 05/01/2013 Daily Email with Text and Picture Attachments	Windowsbeven Forensics <peterwilson.win7@live.com>, "PeterWilson "PeterWilson.Win8@gmail.com" <peterwilson.win8@amail.com>, Windo</peterwilson.win8@amail.com></peterwilson.win7@live.com>	Peter Wilson <peterwilson.win8@live.com> Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com></peterwilson.win8@live.com>	
2013 (127 / 127)		161D7F99-00000016.emi	4/25/2013 10:15:45 P	04/25/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com>, WindowsSeven Forensics <p< td=""><td>peterwilson.win8@gmail.com</td><td></td></p<></peterwilson.win8@live.com>	peterwilson.win8@gmail.com	
B Senders [From] (241 / 241)		1874002C-00000020.eml 35E87F32-00000118.eml	5/4/2013 3:47:16 PM (4/28/2013 4:09:44 PM	05/04/2013 Daily Email 04/28/2013 Daily Email	Peter Wilson <pre>cpeterwilson.win8@live.com>, WindowsSeven Forensics <p WindowsSeven Forensics <peterwilson.win7@mmail.rom>. WindowsSeven</peterwilson.win7@mmail.rom></p </pre>	peterwilson.win8@gmail.com peterwilson.win8@gmail.com	
B-G Recipients [To, CC, BCC] (135/135)		54EE6884-00000011.emi	4/23/2013 10:46:42 P	04/23/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com>, WindowsSeven Forensics <p< td=""><td>peterwilson.win8@gmail.com</td><td></td></p<></peterwilson.win8@live.com>	peterwilson.win8@gmail.com	
Email Domains [2 / 2]		00294823-00000025.eml	5/2/2013 11:08:27 AM	05/02/2013 Daily Email	"Windows7 Live" <peterwilson.win7@live.com>, "Windows8 Gnail" <pete "windows7="" "windows8="" <pete<="" <peter="" <peter.windows7="" gnail"="" live"="" td="" windows7=""><td>Gmail Account <peterwilson.win7@gmail.com> Gmail Account <pre>contourions</pre></peterwilson.win7@gmail.com></td><td></td></pete></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com> Gmail Account <pre>contourions</pre></peterwilson.win7@gmail.com>	
Display Name (135/135) Small Addresses (135/135)		10226134-00000022.emi	5/1/2013 11:34:57 AM	 Re: 05/01/2013 Daily Email with Text and Picture Attachments 	"Live Account" <peterwison.win7@ive.com></peterwison.win7@ive.com>	Gmail Account <peterwison.win7@gmail.com> Gmail Account <peterwison.win7@gmail.com></peterwison.win7@gmail.com></peterwison.win7@gmail.com>	
Endline Email Addresses (135 / 135)		14C00101-0000001D.eml	4/26/2013 11:47:47 A	Fw: 04/26/2013 Daily Email	"Windows7 Live" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	
peterwison.win7@live.com (70 / 70)		188E6784-00000014.eml	4/24/2013 9:31:30 PM	04/24/2013 Email with Attachment 0E02/2013 Date Email	WindowsSeven Forensics <peterwilson.win7@ihve.com>, WindowsSeven WindowsSeven Forensics <peterwilson win7@ihve.com="">, "NetwoWilson</peterwilson></peterwilson.win7@ihve.com>	Peter Wilson <pre>com> Peter Wilson <pre>com> Peter Wilson <pre>com></pre></pre></pre>	
 peterwisch.winsgigmail.com (48 / 48) geterwisch.winsgilwe.com (48 / 48) 		266018E8-00000023.eml	5/1/2013 11:35:14 AM	 Fw: 05/01/2013 Daily Email with Text and Picture Attachments 	"Windows7 Live" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <pre>ceterwilson.win7@gmail.com></pre>	
CC" Recipients (4/4)		2CD672AE-00000015.eml	4/25/2013 9:52:29 PM	04/25/2013 Daily Email	"Windows8 Gmail" <peterwilson.win8@gmail.com>, "Windows8 Live" <pe< td=""><td>Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com></td><td></td></pe<></peterwilson.win8@gmail.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	
Hold Tecc' Recipients (0/0) Hold Tecc' Recipients (0/0) Hold Tecc' Recipients [2/2]		2CD672AE-00000027.eml 2FED7B25-00000024.eml	5/3/2013 4:49:04 PM (5/1/2013 11:41:58 AM	Re: 05/03/2013 Daily Email; 05/01/2013 Daily Email with Text and Picture Attachments	"Live Account" <peterwilson.win7@tve.com> "PeterWilson.Win8@omail.com" <peterwilson.win8@omail.com>, Windo</peterwilson.win8@omail.com></peterwilson.win7@tve.com>	Gmail Account <pre>cpeterwiison.win7@gmail.com> Peter Wilson <pre>cpeterwiison.win8@live.com></pre></pre>	
E I Display Name (135 / 135)		595228A8-00000020.eml	4/28/2013 4:09:44 PM	04/28/2013 Daily Email	WindowsSeven Forensics <peterwilson.win7@gmail.com>, WindowsSev</peterwilson.win7@gmail.com>	peterwilson.win8@gmail.com	
E- Call Email Addresses (135 / 135)	H	5EE25685-00000018.emi	4/25/2013 10:15:45 P	04/25/2013 Daily Email 04/23/2013 Daily Email	Peter Wilson <pre>cpeterwilson.win8@live.com>, WindowsSeven Forensics <p <pre="" peter="" wilcon="">cpeterwilson.win8@live.com>, WindowsSeven Forensics <p< pre=""></p<></p></pre>	peterwison.win8@gmail.com	
		69525F90-00000028.eml	5/3/2013 4:49:35 PM (Fw: 05/03/2013 Daily Email;	"Windows7 Live" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <pre>cpeterwiison.win7@gmail.com></pre>	
		7AA146F3-0000001C.eml	4/26/2013 11:47:32 A	Re: 04/26/2013 Daily Email	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	
		7AP8013D-00000012.emi 0702095E-0000000C.emi	4/23/2013 10:53:02 P 4/26/2013 11:47:47 A	04/23/2013 Daily Email Fw: 04/26/2013 Daily Email	"Windows/ Live" <peterwilson.win @live.com="">, "Windows8 Gmail" <pete "Windows7 Live" <peterwilson.win7@live.com></peterwilson.win7@live.com></pete </peterwilson.win>	Gmail Account <peterwison.win7@gmail.com> Gmail Account <peterwison.win7@gmail.com></peterwison.win7@gmail.com></peterwison.win7@gmail.com>	
		16496DF1-00000011.eml	5/3/2013 4:49:04 PM (Re: 05/03/2013 Daily Email;	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwijson.win7@gmail.com></peterwijson.win7@gmail.com>	
		31751D0E-0000000B.eml 4AE13D6C-00000005 aml	4/26/2013 11:47:32 A 4/24/2013 0-31-30 PM	Re: 04/26/2013 Daily Email 04/24/2013 Email with Attachment	"Live Account" <peterwison.win7@live.com> WindowsSevan Enrangics WindowsSevan</peterwison.win7@live.com>	Gmail Account <pre>cpeterwilson.win7@gmail.com> <pre>pater Wilcon createrwilson.win7@live.com></pre></pre>	
	0	4AE13D6C-00000013.eml	5/3/2013 5:03:28 PM (05/03/2013 Daily Email	WindowsSeven Forensics <peterwison.win?@ive.com>, "PeterWison</peterwison.win?@ive.com>	Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com>	
		4EB5170A-0000000F.emi	5/1/2013 11:41:58 AM	OS/01/2013 Daily Email with Text and Picture Attachments Email: 05/02/2013 Daily Email:	"PeterWilson.Win8@gmail.com" <peterwilson.win8@gmail.com>, Windo</peterwilson.win8@gmail.com>	Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com>	
		625E383D-0000000E.emi	4/28/2013 4:09:44 PM	- w. 05/03/2013 Daily Email	WindowsSeven Forensics <peterwilson.win7@gmail.com>, WindowsSev</peterwilson.win7@gmail.com>	-swaw Account <pre>cpeterwison.wn/@gmail.com> peterwison.win8@gmail.com</pre>	
		6AA5669F-00000003.eml	4/23/2013 10:46:42 P	04/23/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com>, WindowsSeven Forensics <p< td=""><td>peterwilson.win8@gmail.com</td><td></td></p<></peterwilson.win8@live.com>	peterwilson.win8@gmail.com	
		72237042-00000008.emi 08832EA6-000000A.emi	4/25/2013 10:15:45 P 5/3/2013 4:49:35 PM /	04/25/2013 Daily Email Fw: 05/03/2013 Daily Email:	Peter Wilson <peterwilson.win8@live.com>, WindowsSeven Forensics <p "Windows7 Live" <peterwilson.win7@live.rom></peterwilson.win7@live.rom></p </peterwilson.win8@live.com>	geterwilson.win8@gmail.com Gmail Account.kpeterwilson.win7@rmail.com>	
		188E6784-00000008.emi	5/2/2013 11:08:27 AM	. 05/02/2013 Daily Email	"Windows7 Live" <peterwilson.win7@ive.com>, "Windows8 Gmail" <pete< td=""><td>Gnail Account <pre>cpeterwilson.win7@gmail.com></pre></td><td></td></pete<></peterwilson.win7@ive.com>	Gnail Account <pre>cpeterwilson.win7@gmail.com></pre>	
		247F1FEE-00000007.eml	5/1/2013 11:35:14 AM	 Fw: 05/01/2013 Daily Email with Text and Picture Attachments Dev 05/03/2013 Daily Email: 	"Windows7 Live" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <pre>cpeterwison.win7@gmail.com> Gmail Account <pre>cpeterwison.win7@gmail.com></pre></pre>	
		296151F4-00000005.emi	4/28/2013 3:57:27 PM	. 04/28/2013 Daily Email	"Windows? Live" <peterwilson.win?@ilve.com>, "Windows8 Gmail" <pete< td=""><td>Gmail Account <peterwison.win7@gmail.com></peterwison.win7@gmail.com></td><td></td></pete<></peterwilson.win?@ilve.com>	Gmail Account <peterwison.win7@gmail.com></peterwison.win7@gmail.com>	
		20024E1C-00000003.eml	4/26/2013 11:47:32 A	Re: 04/26/2013 Daily Email	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	
		4FE97D3A-00000001.eml 53902427-00000004.eml	4/23/2013 10:53:02 P 4/26/2013 11:47:47 4	04/23/2013 Daily Email Fw: 04/26/2013 Daily Email	'windows/ Live'' <peterwilson.win7@live.com>, 'Windows8 Gmail' <pete 'Windows7 Live'' <peterwilson.win7@live.com></peterwilson.win7@live.com></pete </peterwilson.win7@live.com>	 umai Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com> Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com> 	
		69525F90-00000002.eml	4/25/2013 9:52:29 PM	04/25/2013 Daily Email	"Windows8 Gmail" <peterwilson.win8@gmail.com>, "Windows8 Live" <pe< td=""><td>Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com></td><td></td></pe<></peterwilson.win8@gmail.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	
		7998735E-00000006.emi	5/1/2013 11:34:57 AM	Re: 05/01/2013 Daily Email with Text and Picture Attachments Confirm your Twitter account Wer7Exercise1	"Live Account" <peterwison.win7@live.com> Windows 7 Forensics https://www.com</peterwison.win7@live.com>	Gmail Account <peterwison.win7@gmail.com> Twitter <p-conversionities twn7="</td"><td>odma-te-</td></p-conversionities></peterwison.win7@gmail.com>	odma-te-
		00294823-00000006.eml	4/21/2013 4:38:09 PM	. 04/21/2013 Daily Email	Windows8 Gmail <peterwilson.win8@gmail.com>, Windows5even Forens</peterwilson.win8@gmail.com>	Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com>	
	1						
ls sent from this acc	our	nts were	sent to a	ccounts that I created	for the purpose of data	generation:	
Is sent from this acc	OUI	nts were	sent to a	ccounts that I created	for the purpose of data	generation:	
Is sent from this acc	OUI	search volate	sent to a	counts that I created	I for the purpose of data g	generation:	× 1
Is sent from this acc	our	search volatie	sent to a	CCOUNTS that I created	I for the purpose of data a	generation:	- 2
Is sent from this acc Explore forwarders' that Graphics Boolmarks Live Sea The all them The Trad State The Constructions The Constructions T	our	serch Volate	sent to a	Counts that I created	I for the purpose of data a tern Sander Time (from local modere) To "Moderary Low" offeet relians work@ins come, "windows Good" offeet.	generation:	- 2
Is sent from this acc Exple Overley 'trail Graphic Bodmark [ue Sar Enal Res Construction of the Construction of the Construction Construction of the Construction	our	Search Volatie Image: Search Volatie	sent to ac	CCOUNTS THAT I Created	I for the purpose of data a standard Time (from local modine) To "Woldword Due" - Geter Wilson, Won 2014er, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Comp Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Comp Terretory, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Comp Terretory, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Comp Terretory, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Comp Terretory, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windows Comp Terretory, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windows Comp Terretory, - Windowse Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windows Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windows Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windows Gaud" - Erten "Windows Due" - Geter Wilson, Won 2014er, - Windows Gaud" - Erten	generation:	• 2
Is sent from this acc	our	Search Volatie Search Volatie Name 00294627-00000025.eml 10263137-00000025.eml 140000105.eml 140000102.eml 140000002.eml	sent to ac sometime sometime sometime spices side sometime spices sometime sometim sometime sometime sometime sometime sometim	Cocounts that I created	I for the purpose of data g	generation:	¥ 2
Is sent from this acc		Name 00244823-0000025.eml 00244823-0000025.eml 1026319-0000022.eml 1260319-0000002.eml 2560728-00000025.eml 2560728-00000025.eml	sent to ac	Cocounts that I created Constant - Depley Time Zone: East Constant - Depley Time Zon	I for the purpose of data g ten Sanded Time (Pronisci notine) To "Windows Une" GeterVision, WinDigites, como, "Windows Ginal" Geter" Windows Une" GeterVision, WinDigites, como, "Windows Ginal" Geter "Windows Une" GeterVision, WinDigites, como, " Windows Une" GeterVision, WinDigites, como, " Windows Une" GeterVision, WinDigites, como, " Windows Une" GeterVision, WinDigites, como, "	generation: Fon Gala Kourt opterwison we?@puid.com Gala Kourt opterwison we?@puid.com Gala Kourt opterwison we?@puid.com Gala Kourt opterwison we?@puid.com Gala Kourt opterwison we?@puid.com	8 2
Is sent from this acc Explore forwarder that Graphics Boolmarks (breaker Examines (breaker) The final State The final Archives The final Arch		the second	sent to ac signature Sizions Time Sizions Time Sizions 10:457 M 4/26/2013 11:4547 M 4/26/2013 11:4547 M 4/26/2013 11:4547 M 4/26/2013 11:4547 M 4/26/2013 4:4504 M 4/26/2013 4:4	Cocounts that I created	I for the purpose of data a standard Time (from local modifier) To "Webword Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?@Hen.com, "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?", wein?", wein?", "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?", wein?", wein?", "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?", wein?", wein?", "Windows® Grad" - deter "Windows? Due" - deter Wilson, Wein?", wein?", wein?", "Windows? Due" - deter Wilson, Wein?", wein?", "Windows?", "Windows® Grad" - deter "Windows?", "Windows?	contractions:	* 1
Is sent from this acc		Nets Were Start Start Walds	Sent to ac Start Tre Sizer Tre <t< td=""><td>Cocounts that I created</td><td>I for the purpose of data a set of the purpose of the set of the purpose of the set of th</td><td>generation:</td><td><u>* 1</u></td></t<>	Cocounts that I created	I for the purpose of data a set of the purpose of the set of the purpose of the set of th	generation:	<u>* 1</u>
Is sent from this acc		Nume Control Control <thcontrol< th=""> <thcontrol< th=""> <thcont< td=""><td>Comparison of the second second</td><td>Cocounts that I created Counts that I count that Counts that Count</td><td>I for the purpose of data a set of the purpose of data a set of the from local moders) To More and The from local moders) To More and the from local moders More and the from loca</td><td>Prom Final Final Final Accurt opterwiskon.witr?@pail.com Ginal Accurt opterwiskon.witr?@pail.com</td><td><u>s /</u></td></thcont<></thcontrol<></thcontrol<>	Comparison of the second	Cocounts that I created Counts that I count that Counts that Count	I for the purpose of data a set of the purpose of data a set of the from local moders) To More and The from local moders) To More and the from local moders More and the from loca	Prom Final Final Final Accurt opterwiskon.witr?@pail.com Ginal Accurt opterwiskon.witr?@pail.com	<u>s /</u>
Is sent from this acc		Search (videle Compared and a second secon	Seent to ac Submt Time Signet T	Cocounts that I created	I for the purpose of data a set of the purpose of data a set of the purpose of data a set of the se	contractions:	× 2
Is sent from this acc		New Control Control <thcontrol< th=""> <thcontrol< th=""> <thcontr< td=""><td>Comparison of the second second</td><td>Cocounts that I created</td><td>I for the purpose of data a ten Standard Time (from local modine) To "In Monto Unit" offer relativity (from local modine) To "Windows Unit" offer relativity (from local modine) "Windows Unit" offer relativity (from local mo</td><td>generation: Tom Tom Tod Accura optendon wi70ppad.com Grait Accura optendon wi70ppad.com</td><td><u>* 1</u></td></thcontr<></thcontrol<></thcontrol<>	Comparison of the second	Cocounts that I created	I for the purpose of data a ten Standard Time (from local modine) To "In Monto Unit" offer relativity (from local modine) To "Windows Unit" offer relativity (from local modine) "Windows Unit" offer relativity (from local mo	generation: Tom Tom Tod Accura optendon wi70ppad.com Grait Accura optendon wi70ppad.com	<u>* 1</u>
Is sent from this acc		Also Wate Search Wate Wee Wee 002942-0000005.ed Wee 002942-000005.ed Wee 002942-000005.ed Wee 00295284-0000005.ed <td< td=""><td>Control of the second sec</td><td>Cocounts that I created Counts that I create</td><td>Loor the purpose of data</td><td>generation:</td><td><u>• 1</u></td></td<>	Control of the second sec	Cocounts that I created Counts that I create	Loor the purpose of data	generation:	<u>• 1</u>
Is sent from this acc		Name Control Control <thcontrol< th=""> <thcontrol< th=""> <thcont< td=""><td>sent to at *(#*) Salar the Status to at Salar the Salar the Salar</td><td>Cocounts that I created</td><td>I for the purpose of data a second time (from local machine) In Mindows' Dia" Geter Vision, WonGlein, como, "Windows' Ginal" Geter, "Windows' Dia" Geter Vision, WonGlein, como, "Windows' Ginal" Geter, "Windows' Dia" Geter Vision, WonGlein, como, "Windows' Dia" Geter Vision, WonGlein, como,</td><td>Contract optimization with Tigenal con- field Accurat optimization</td><td>• 1</td></thcont<></thcontrol<></thcontrol<>	sent to at *(#*) Salar the Status to at Salar the Salar	Cocounts that I created	I for the purpose of data a second time (from local machine) In Mindows' Dia" Geter Vision, WonGlein, como, "Windows' Ginal" Geter, "Windows' Dia" Geter Vision, WonGlein, como, "Windows' Ginal" Geter, "Windows' Dia" Geter Vision, WonGlein, como,	Contract optimization with Tigenal con- field Accurat optimization	• 1
Is sent from this acc		New Control Control <thcontrol< th=""> <thcontrol< th=""> <thcontr< td=""><td>Seent to ac ************************************</td><td>Cocounts that I created</td><td>I for the purpose of data a set of the purpose of data a set of the purpose of data a set of the purpose of the set of th</td><td>generation:</td><td><u>s 2</u></td></thcontr<></thcontrol<></thcontrol<>	Seent to ac ************************************	Cocounts that I created	I for the purpose of data a set of the purpose of data a set of the purpose of data a set of the purpose of the set of th	generation:	<u>s 2</u>
Is sent from this acc		Net Object 002462-0000005.ed 002462-0000005.ed 002462-0000005.ed 002462-0000005.ed 002462-0000005.ed 002462-0000005.ed 00254726-0000007.ed 00254726-0000007.ed 00254726-0000007.ed 00255476-0000007.ed 00254726-0000007.ed 00255476-0000007.ed 00254726-0000007.ed 00255476-0000007.ed 00255476-0000007.ed 00255476-0000007.ed 00255476-000007.ed 00255476-000007.ed 00255476-000007.ed 00255476-0000007.ed	Seent to at \$2000 11:00:274 \$2000 11:0	Cocounts that I created	Locat Check purpose of data Constraints and the Constrai	generation:	<u>a</u>
Iss sent from this acc Eater Counterwy Chail Count Counterwy Total Ener Counterwy Chail Counterwy		Alts Weate Stard Weate Wate Weate Weate We	Seent to al *(#*) Solar time Status to al Solar time Status to al Solar time Status to al Solar time Status to al Status to al Stat	Cocounts that I created	I for the purpose of data a grant of the purpose of data a grant of the purpose of data a grant of the purpose	peneration:	<u>a A</u>
Is sent from this acc		Alts Weater Search Weater Image Image Displez2-0000025.ell Image Displez2-0000005.ell Image	Seent to ac 	Cocounts that I created	Bron the purpose of data Constraints Const	peneration:	8 2
Is sent from this acc		Association Search Wate Search Wate Search Search Search Wate Search Search Search Search Search Search	Seent to au Seent to au Sector 100 Sector 100 Sect	Cocounts that I created	Local Television Medigies cans, "Mediand Graff Ortex, Mediand Tani, from Inclaimadree) To Mindow Tani, "Ortex Median, Medigies cans, "Mediand Graff Ortex, Mediand Tani, "Ortex Median, Medigies, cans, "Mediand Graff, Ortex, Mediand Tani, "Ortex Median, Medigies, cans, "Mediand Graff, Ortex, Mediand Tani, "Ortex Median, Medigies, cans, Mediand Graff, "Ortex Median, Median, cans, Mediand Graff, "Ortex Median, Med	Form Final Accurt speteriolox wit70pula cost onal Accurt speteriolox wit70pula cost	<u>a A</u>
Ls sent from this acc Teal ten teal teal ten teal teal teal teal teal teal teal teal		Alts Weate Stard Weate Wate Weate <	Seent to al *(#*) Solar time Status to al Solar time Solar time	Cocounts that I created	Bond the purpose of data Constraints of the purpose of data Constraints of the purpose of data Constraints of the purpose of the purpose of the purpose Constraints of the purpose of the purpose Constraints of the purpose of the purpose Constraints of	energia de la constructione a la	<u>s 2</u>
Is sent from this acc		Also Wate Search Wate Wei Wei D029425-0000005.ell Wei D029426-0000007.ell Wei D029427-0000007.ell Wei D029427-0000007.ell Wei D029427-0000007.ell Wei D029427-000007.ell Wei D029427-000007.ell Wei D029427-000007.ell Wei D029427-0000007.ell Wei	Sent to ac Sent to ac Sector Tree Sizent Tree Sizent Tree Sizent Tree Sizent Tree Sizent Tree Sizent Tree Sizent Tree Sizent Sizen	Cocounts that I created	the standard Time (from local machine)		<u> </u>
Is sent from this acc		Association Search Walf Search Walf Search Search Walf Search Old Performance Search Search Old Performance Search Search Old Performance Search Search Old Performance Search Search Schold Perfo	Seent to au Sector to au Sec	Cocounts that I created Cocounts that I crea	Local Control of the purpose of data as a second seco	Construction C	o 2
Is sent from this acc		Alts Weate Search Weate Wine Weate Weate Weate Weate <td< td=""><td>Seent to al - (#*) (2 Sdort Time St2013 1: 0627 AH - (1202013 1: 0627 AH - (1202013 1: 0627 AH - (1202013 1: 0527 AH - (1202013 1:</td><td>Cocounts that I created</td><td>Bond the purpose of data Constraints of the purpose of data Constraints of the purpose of data Constraints of the purpose of the purpose of the purpose Constraints of the purpose of the purpose Constraints of the purpose of the purpose Constraints of</td><td>energia de la construcción de la</td><td><u>a</u></td></td<>	Seent to al - (#*) (2 Sdort Time St2013 1: 0627 AH - (1202013 1: 0627 AH - (1202013 1: 0627 AH - (1202013 1: 0527 AH - (1202013 1:	Cocounts that I created	Bond the purpose of data Constraints of the purpose of data Constraints of the purpose of data Constraints of the purpose of the purpose of the purpose Constraints of the purpose of the purpose Constraints of the purpose of the purpose Constraints of	energia de la construcción de la	<u>a</u>
Is sent from this acc		Net Object 029427 0246 029427 029427 029427 020427 029427 020427 029427 02000023 029427 02000023 02057247 0000015 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 0000012 02057247 00000012 02057247 00000012 02057247 00000012 02057247 00000012 02057247 00000012 02057247 00000012 02057247 00000012 02057247 00000012 0205724	Sent to au Sent to au Second Time Sizona	Cocounts that I created	I for the purpose of data a general sector of the sector o	peneration:	× 2
Is sent from this acc		Control (Control (Contro) (Control (Contro) (Control (Contro) (Contro) (Contro) (Contro)	Seent to au Sector to au Sec	Cocounts that I created Cocounts that I crea	Brown the purpose of data a Constraint of the purpose of data a Constraint of the purpose of data a Constraint of the purpose of the purpose Constraint of the purpose of the purpose Constraint of the purpose of the purpose Constraint of the purpos	Pon Final Accurar optierelicou wir70pril accord final Accurar op	<u>a</u>
Is sent from this acc		Alts Wate Search Wate Image Image Image	Sent to al Source the Source	Cocounts that I created	Bonderd Time (from local machine) In Standard Time (from local machine) In "Webword Due" deter Wildon, Weißflew, comp., "Windows Goad" deter, Windows Due" deter Wildon, Weißflew, comp.	eneration: fon fon fon fon fon fon fon fon	<u>o 2</u>
Is sent from this acc		Also worker: Search Walk Image: Image: Image: Image:	Seent to al Sector to al Sizent the Sizent the Sizent the Sizent the Sizent the Sizent to	Cocounts that I created	In the second se	Energical contractions and the second	× 2
Is sent from this acc		Also worker: Start Start Walk Wei Wei CONSTRUCT	Sent to au Sector to au Sect	Cocounts that I created	Effort the purpose of data age Enclosed Time (from local machine) To To To		<u>s 0</u>
Is sent from this acc		Also were :: Search Walk	Sent to ac Sector to ac Sect	Coounts that I created	the second		× 2
Is sent from this acc		Also were: Search Wate Search Wate Wate Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Compariso	Sent to ac Sector to ac Sect	Cocounts that I created	Control of the purpose of data of the second s	Per Contrasting operations and	<u> </u>
Is sent from this acc		Also were : Search Walls Search Walls Search Walls Search Walls Search Walls Search Search	Sent to ac Sector ac	Coounts that I created Coount	the second	Pan Markatara spetradox antibipata con cala kozara spetradox antibipata cala	<u> </u>
Is sent from this acc		Alts Weite Search Search Search <td< td=""><td>Sent to ac </td><td>Coounts that I created</td><td>the sended Time (free had medine)</td><td>energina de la construction de l</td><td></td></td<>	Sent to ac 	Coounts that I created	the sended Time (free had medine)	energina de la construction de l	

L

Explore Overview Email Graphics Bookmarks Live Sea						
Email Rems 4.0	File List		e 🗢 🔟 curt	me Zone: Fastern Standard Time (From Incel marhine)		- - -
Email Status		Sidenit Timo	Subject		Erom	8 ax
E Email Archives	00294823-00000012 et	4/24/2013 9-14-02 DM	04/24/2013 Email with Attachment	"Windows? Goal" < Reterillion Win?@omail.com > "Windows? Goal" < R	"Two formunt" «Detervitikon Win7filikus com»	
B Submitted (237/237)	00294823-00000012.en	5/3/2013 4:35:29 PM /	05/03/2013 Daily Email:	 Windows7 Gmail: Windows7 Gmail: Peter/Wison.Win7/Birmail.com >: 'Windowc8 Gmail' Peter/Wison.Win7/Bir	"Live Account" «PeterWikon.Win7@ive.com»	
E- Delivered (127 / 127)	0E1C7415-0000001C.er	5/1/2013 11:19:43 AM	. 05/01/2013 Daily Email with Text and Picture Atta	hments "Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p.< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p.<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
E-2013 (127 / 127)	13F27855-00000019.en	4/26/2013 11:32:21 A	04/26/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
E-Lati Effail Addresses	18F9282F-00000010.en	4/21/2013 3:53:37 PM	. 04/21/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
E Cal Email Domains [8/8]	258A0803-00000014.er	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email	"Gmail Account" <peterwiison.win7@gmail.com></peterwiison.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
Display Name (241 / 241)	00294823.00000016.em	4/25/2013 10:08:24 P	Pw: 04/25/2013 Daily Email	'Grail Account', caeterwison, win7/ligmail.com>	Twe account: «Peterwison win/igive.com»	
⊟ Email Addresses (241 / 241)	123836DD-0000001B.er	4/26/2013 11:32:21 A	04/26/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p.,< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p.,<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
 (none) (106) 106) (and confirm+accs/0zs/3awszb24ud2lun0bobwfol 	168B3DAB-00000010.er	4/21/2013 3:53:37 PM	. 04/21/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p.< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p.<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
mail-noreply@google.com(6/6)	188E6784-00000013.en	i 4/24/2013 9:14:02 PM	. 04/24/2013 Email with Attachment	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
- The member_services@live.com (1/1)	188E6784-00000026.en	5/3/2013 4:35:29 PM (05/03/2013 Daily Email;	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
 In-orgrejvyfba.jva7=yvir.pbz-299c4@postmi accessio.475bs/206@sks.accedo.com (8 / 8) 	23006APT-00000017.er	4/25/2013 10:06:24 P 5/11/2013 11:19:43 AM	05/01/2013 Daily Email with Text and Picture Atta	hments "Windows7 Gmail" «PeterWilson Win7@gmail.com> "Windows7 Gmail" «PeterWilson Win7@gmail.com> "Windows8 Gmail" «P	Twe account "Peterwison win/gave.com>	
- Inoreply-473bacs/replus.google.com (2 / 2)	188E6784-00000006.en	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email	"Gmail Account" <pre>cpeterwilson.win7@gmail.com></pre>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
- Cal notification+kr4yybkynkma@facebookmail.o	4AE13D6C-00000004.er	il 4/24/2013 9:14:02 PM	04/24/2013 Email with Attachment	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
peterwilson.win7@gmail.com (35 / 35)	4AE13D6C-00000010.er	nl 5/3/2013 4:35:29 PM (. 05/03/2013 Daily Email;	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
 Determision.win7(Elive.com (27 / 27)) Retermision.win9(Servel.com (16 / 16)) 	5280174E-00000002.en	4/21/2013 3:53:37 PM	. 04/21/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p.< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p.<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
- Determision.win8@live.com (16/16)	60022000000000000000000000000000000000	4/25/2013 11:32:21 A 4/35/2013 10:09:24 B	04/25/2013 Daily Email Even 04/25/2013 Daily Email	"Windows/ Ginal" <peterwision.win lggmail.com="">, "windows/ Ginal" <p "windows="" <peterwision.win="" ginal"="" lggmail.com="">,</p></peterwision.win>	"Live Account" <peterwillion.win ligitye.com=""></peterwillion.win>	
- 🔄 pjw6578@vit.edu (4 / 4)	01294823-0000003.es	4/25/2013 10:08:24 P	Re: 04/25/2013 Daily Email	"Gravi Account" contentinon win78pmail.com>	"Live Account" «PeterWison Win7@ive.com>	
- Call update+kr4yybkynkma@facebookmail.com (00294823-00000007.en	5/3/2013 4:35:29 PM (05/03/2013 Daily Email;	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
	188E6784-00000001.en	4/21/2013 3:53:37 PM	. 04/21/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
(E. (20 Engli (244) 244)	188E6784-00000004.en	4/25/2013 10:08:24 P	Fw: 04/25/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
	188E6784-00000005.en	4/26/2013 11:32:21 A	04/26/2013 Daily Email	"Windows7 Gmail" <peterwilson.win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
	69525F90-00000006.en	5/1/2013 11:19:43 AM	 05/01/2013 Daily Email with Text and Picture Attain or Instance of the Instance o	hments Windows7 Gmail < PeterWilson.Win7@gmail.com>, "Windows8 Gmail" <p< td=""><td>"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com></td><td></td></p<>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	
	1A062209-00000002.8	 	. Org24/2013 Einde wich Actacianent	windows/ dinal Crecer wison, win/ gigital, collizy, windowse dinal Cr.	Live Account Crecer Historic Historic Comp	
د 2	Loaded: 27 Fittered:	27 Total: 27 e 39 Ema	[Hallighted: 0 [Chedded: 0	Tourise: 563418 erwilson.win7@live.com		
FTK found a to eiver was either peter	Figur Figur tal of 15 en wilson.win	27 Tool: 27 e 39 Ema nails that 7@gmial	ill sent from pet were forwards of .com or peterwil	Produces 55510 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	ll of the emails,	the
FTK found a to eiver was either peter	Figure tal of 15 en wilson.win	²⁷ [1446-27 e 39 Ema nails that <u>7@gmial</u>	(Hyperson of Desterior) iii sent from pet were forwards of .com or peterwil	Produces 195910 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	ll of the emails,	the
FTK found a to eiver was either peter	Tigur Figur tal of 15 en wilson.win	²⁷ [1686.27 e 39 Ema nails that <u>7@gmial</u>	ill sent from pet were forwards of .com or peterwil	President 665410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	ll of the emails,	the
FTK found a to eiver was either peter	Tigur Figur tal of 15 en wilson.win	27 [totak 27 e 39 Ema nails that 7@gmial	Iteration Iteration nil sent from pet were forwards or .com or peterwil	TreatIsee 565/10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: • Digday Time Zone: Eastern Standard Time (from local machine)	ll of the emails,	the
FTK found a to eiver was either peter	Figure Figure tal of 15 en wilson.win research Index Search Vol Control C	27 Total: 27 e 39 Ema hails that 7@gmial http://www.state.org/linearized/li	Implement 0 Observed 0 Ail sent from pet were forwards or .com or peterwill Steer	FreatSee: 555110 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: . topslay Time Zone: Eastern Standard Time (from local machine)	ll of the emails,	the
FTK found a to eiver was either peter	Tigur Figur tal of 15 en wilson.win	27 Taxi: 27 e 39 Ema hails that 7@gmial te	Hyddyted 0 (Decide 0) nil sent from pet were forwards or .com or peterwil Sket B340	Treatisee 565/10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com; • topslay Tme Zone: Eastern Standard Time (from local machine) Top * topslay Tme Zone: Eastern Standard Time (from local machine) Top * topslay Time Zone: Eastern Standard Time (from local machine)	Ill of the emails,	the
FTK found a to FTK found a to eiver was either peter Englitens	Tigur Figur tal of 15 en wilson.win	27 [Total: 27 e 39 Ema nails that <u>7 @ gmial</u> the 15.set 4/252031310.	Image: product of the sent from pet ail sent from pet were forwards or .com or peterwil Sobject Sobject Sobject	Treatise: 505/10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: . Diglay Time Zone: Eastern Standard Time (From local machine) To "Window? Const" - detertwinkon.win2@gogad.com	Ill of the emails,	the
FTK found a to FTK found a to eiver was either peter Endre Overvey End Graphis Bookmats End Atashmets (010) End Atashmets (010) End Repk (18) (10) End Repk (18) (15) End Repk (18) (15)	Figure Figure tal of 15 en wilson.win ve Search Index Search Vol Figure tal of 15 en wilson.win	27 [Total: 27 e 39 Ema nails that 7 @ gmial the 15.em 4/25/2013 10- 105.em 4/25/2013 10-	Hydrighted 0 Checked 0 Aill sent from pet were forwards o: .com or peterwil State State State Mark Science State	TerailSite: 565/10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com; • Display Time Zone: Eastern Standard Time (from local machine) To "Windows? Gmail" deterwilson, Win?@gmail.com "Windows? Gmail" deterwilson, Win?@gmail.com	Ill of the emails,	the
FTTK found a to FTTK found a to eiver was either peter End Rens End Ratachinets (0/0) End Related tens (From End) (584/0) End Related tens (From End) (584/0)	Tigur Figur tal of 15 en wilson.win ve Search 10de Search 10de Ve Search 10de Sea	Total: 27	Image: Provide a constraint of the section of the	Treatises: 500-100 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com; • Display Time Zone: Eastern Standard Time (From local machine) To *Window? Gmail "deterWiston, Win7@gmail.com *Window? Gmail" deterWiston, Win7@gmail.com	Ill of the emails,	the
FTK found a to FTK found a to eiver was either peter Enal Hos Enal Attachments (0 / 0) Enal Reded Hens (Fron Enal) (59 / 0)	Tigur Figur tal of 15 en wilson.win ve Search Index Search Vol 14/C00101-0000 2 5001889-00000 2 500189-00000 2 500189-0000 2 500189-0000 2 500189-0000 2 500189-0000 2 500189-0000 2 50019-0000 2 50019-0000 2 50019-0000 2 50019-0000 2 50019-0000 2 50019-0000 2 50000 2 50019-0000 2 50000 2 500000 2 50000 2 50000 2 5000000 2 500000	17 Total: 27 e 39 Ema anails that 7 @ gmial stat 101.em 4/25/2013 10: 101.em 4/25/2013 10: 101.em 4/25/2013 10: 101.em 4/25/2013 10: 102.em 5/1/2013 10: 23.em 5/1/2013 10:	INPRESENT Otherade 0 Aill sent from pet were forwards of .com or peterwill Subject Subject State Person Frei Off/2013 Daty Email State Person S	TearlSee: 555110 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	Ill of the emails,	the
FTK found a to FTK found a to eiver was either peter Enal Items Enal Items (For Enal (15/15) Enal Related Items (for Enal) (59/10) Enal Related Items (for Enal) (59/10)		Total: 27	Highlighted 0 Checkled 0 ail sent from pet were forwards or .com or peterwil Bize R Final Sobject Bize R Final State H Final (State) Email	TrailSee 503-118 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	Ill of the emails, Ill ve Acourt '-PeterWison.wh76 'Tran ' We Acourt '-PeterWison.wh77 Gial Acourt - cpterwison.wh78 Gial Acourt - cpterwison.wh78 Gi	the Plve.com> gmai.com> gmai.com> gmai.com> gmai.com>
FTK found a to FTK found a to eiver was either peter Ealters End State End Mathematic (10) End Mathematic (10) End Robert (18) End Rob		17 Total: 27 e 39 Ema anails that 7@gmial anails 10cm 4/25/2013 10:4	INSTRUCT Obstact:0 ail sent from pet were forwards or .com or peterwill Subject Sobject	Treatise: 555/10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: . toplay The Zone: Estern Standard Time (from local machine) 10 "Window? Gmail" -DeterWinn: Win7@gmal.com "Window? Gmail" -DeterWinn: Win7@gmal.com "Window? Gmail" -DeterWinn: Win7@gmal.com "Window? Ind" -DeterWinn: Win7@gmal.com "Window? Und" -DeterWin	Ill of the emails, Ill of the emails, From ¹ Ure Accourt "deterwison win7% Grial Acourt opterwison win7%	the
FTK found a to FTK found a to eiver was either peter Enal items Enal items Enal items (1010) Enal Related tems (from Enal) (58+10) Enal Related tems (from Enal) (58+10) Enal Related tems (from Enal) (58+10) Enal Address Enal Address Enal Address Enal Address Enal Address Enal Address Enal Address Enal Address		27 [Text: 27 e 39 Ema hails that 7@gmial Me 5.54mt Time 4.55203 10 10.54mt 4.55203 10 10.540mt 4.55203 10 10.5500 10 10000 10 10.55000 10000 1000000000000000000000000		TrailSite 50x10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: Display Time Zone: Eastern Standard Time (Pron local machine) In *Vindows7 Gmil" @eter Wilson.Win7@gmal.com *Vindows7 Jume" #eter Wilson.Win7@gmal.com	Ill of the emails,	the Networks N
FTK found a to FTK found a to eiver was either peter Explore overvey Enal Grachts Boolmarks Final Items Final Atachmert (0 (0) Final Atachmert (Total: 27	Hydrighted: 0 Obsided: 0 aill sent from pet were forwards or .com or peterwill .big: 0 Final .sobget .sobget .sobget .sobget	Tradition: 565410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	Ill of the emails, Ill of the em	the viewscom> gmai.com> gmai.com> gmai.com> gmai.com> gmai.com> gmai.com> gmai.com>
FTK found a to FTK found a to eiver was either peter End Ros End Ros E		Texel: 27 Texel: 27 Texel: 27 e a39 Emai anails that 7@gmial state Submet Time // Constant // Con	Highlighted 0 Checkled 0 ail sent from pet were forwards or .com or peterwill Stape:	TrailSiere 500-110 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: to to to to to to to to to	Ill of the emails, Ill of the emails, From From From From From From From From	the weight of the second productions prod
FTK found a to FTK found a to eiver was either peter End tens End Adachmets (0 / 0) End		Total: 27	Hydrighted: 0 Obseld: 0 sill sent from pet were forwards or com or peterwill Sobject Sobject <td>Tradition: 505410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: • Diglay Time Zone: Eastern Standard Time (from Iscal machine) In *Window? Cond" deterWinco.Win7@pan.com *Window? Cond" deterWinco.Win7@pan.com *Window? Cond" deterWinco.Win7@pan.com *Window? Line" deterWinco.Win7@pan.com</td> <td>Ill of the emails, Ill of the em</td> <td>the</td>	Tradition: 505410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: • Diglay Time Zone: Eastern Standard Time (from Iscal machine) In *Window? Cond" deterWinco.Win7@pan.com *Window? Cond" deterWinco.Win7@pan.com *Window? Cond" deterWinco.Win7@pan.com *Window? Line" deterWinco.Win7@pan.com	Ill of the emails, Ill of the em	the
FTK found a to FTK found a to eiver was either peter End Items End Machine (10) End Machine		r Texel: 27 e 39 Emai e 39 Emai hails that 7 @ gmial te	Highlighted 0 Checklind 0 ail sent from pet were forwards or com or peterwill file file <td>Traditione 565410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: tgpleyTmeZone:EasternStandard Time (from local machine) tg vindows/Lue⁴ Orbert Wilson.Win7@live.com vindows/Lu⁴ Orber</td> <td>Ill of the emails, Ill of the emails, Interpretation of the emails, Interpretation of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails of the emails Interpretation of the emails of the e</td> <td>the Nive.com> gmai.c</td>	Traditione 565410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: tgpleyTmeZone:EasternStandard Time (from local machine) tg vindows/Lue ⁴ Orbert Wilson.Win7@live.com vindows/Lu ⁴ Orber	Ill of the emails, Ill of the emails, Interpretation of the emails, Interpretation of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails Interpretation of the emails of the emails of the emails of the emails Interpretation of the emails of the e	the Nive.com> gmai.c
FTTK found a to FTTK found a to eiver was either peter End Rens End Ratachnets (0 / 0) End Ratachnets (0 / 0) End Related tens (From End) (584 / 0) End (584 / 244 / 244)		Total: 27	Hydrighted 0 Othersded 0 ail sent from pet were forwards or	Tradition: 500-100 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com; . Display Time Zone: Eastern Standard Time (From Iscal machine) To "Windows? Conal" deterWisco. Win7@bes.com> "Windows? Une" deterWisco. Win7@bes.com> "Wi	Ill of the emails, Ill of the emails, From Vie Acourt "deterWion.Wir76 Gial Acourt opterwion.wir79 Gial Acourt opterwion.wir79	the when coms predictors p
FTTK found a to FTTK found a to eiver was either peter End Itens End Itens End Atexhos End Atexhos	Index Search Index Index Search Index Search Index Search Index Se	27 Texel: 27 e 39 Emai e 39 Emai hails that 7 @ gmial tec	Highlighted 0 Other Side atil sent from pet were forwards or com or peterwill file file <td>Traditioner 565410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com; typesty The Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Control of the Standard Million Control of the Million Million Control of Million Control of the Million Million Control of Million Control of</td> <td>Ill of the emails, Ill of the emails, From > The Accourt opterwise, mi78 Grad Accourt opterwise, mi79 Grad Accourt opterw</td> <td>the where com- grad com- grad</td>	Traditioner 565410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com; typesty The Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Eastern Standard Time (from local machine) typesty Time Zone: Control of the Standard Million Control of the Million Million Control of Million Control of the Million Million Control of	Ill of the emails, Ill of the emails, From > The Accourt opterwise, mi78 Grad Accourt opterwise, mi79 Grad Accourt opterw	the where com- grad
FTK found a to FTK found a to eiver was either peter End Ratedmarks (0/0) End Ratedm		Texes: 27	Highlighted 0 Otherside 0 ail sent from pet were forwards or	TrailSite: 503-118 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: Clipplay The Zone: Eastern Randed The (from local machine) Clipplay The Zone: Eastern Randed The (from local machine) Clipplay The Zone: Eastern Randed The (from local machine) Clipplay The Zone: Eastern Randed The (from local machine) Clipplay The Zone: Clipplay	Ill of the emails, Ill of the em	the where the where the where the where the where the where the where the wher
FTK found a to FTK found a to eiver was either peter For every End @copies Bookmats For al Atsommets (0 / 0) For al A		Texel: 27	Heighteted 0 Obesided 0 atil sent from pet were forwards or .com or peterwill .c	Installates 565/10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: • Display Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Eastern Standard Time (From local machine) • Unsplay Time Zone: Grad (Fragmachine) • Unsplay Time Zone	Ill of the emails, Ill of the emails, Ill of the emails	the weak of the second
FTK found a to FTK found a to eiver was either peter Enal Ites Enal Ites Enal Address Enal Address Enal Address Enal (244/244)	Index Search (%) Ind	27 [Texel: 27 e 39 Emails hails that 7 @ gmial the 105-em 145/2013 11: 102-em 145/2013 11: 102-em 14	Highlighted. 0 Otherside 0 adil sent from peter were forwards or	TerailSite: 50x10 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f previously sent emails. In a son.win7@live.com to a son.win7@live.	Ill of the emails, Ill of the emails, Ill of the emails, From From From From From From From Grait Accourt opterwison.win78 Grait Accourt opterwison.win78 Grait Accourt opterwison.win78 Grait Accourt opterwison.win79 From Accourt op	the construction of the co
FTK found a to eiver was either peter Explore Overvey End Graphics Bookmarks End Items End Matachmerts (0 / 0) End Matachmerts	test of the second	27 Total: 27 e 39 Ema basis that 7@gmial the 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Hydrighted: 0 Obseld: 0 ail sent from pet were forwards or com or peterwill biper biper biper <td>TerailSee: 593418 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f provide for all 'detartion of the son of the</td> <td>Ill of the emails, Ill of the em</td> <td>the and a second second</td>	TerailSee: 593418 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f provide for all 'detartion of the son of the	Ill of the emails, Ill of the em	the and a second
FTK found a to eiver was either peter End tots End Advancets (0 /0) End (0 /0) E	Index Search Index Index Search Index Search Index Search Index Se	27 Texel: 27 e 39 Emails chails that 7 @ gmial the 5 down in the 5 down	Highlighted. 0 Otherside 0 still sent from peter were forwards or com or peterwill difference difference <td>Tear User Store</td> <td>Ill of the emails, Ill of the emails, From From From From From From From From</td> <td>the where com- grad com- grad</td>	Tear User Store	Ill of the emails, Ill of the emails, From From From From From From From From	the where com- grad
FTK found a to eiver was either peter End Rens End Ratachnets (0 / 0) End Ratachnets (0 / 0	Index 39 - 1 - 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2	27 Total: 27 e 39 Emails chails that 7 @ gmial the 7 @ gmial the 7 @ gmial the 7 @ gmial 055.em 7 (25/2013 11:0 177.em 7 (25/2013 11:0 17	Hydrighted: 0 Othersdel 0 ail sent from pet were forwards or com or peterwill 00000 00000 </td <td>TerailSee: 593-119 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f previously sent emails. In a son.win7@live.com f previously com f of the set of t</td> <td>Ill of the emails, Ill of the emails, Ill of the emails, Ill of the emails</td> <td>the Wescons predictore</td>	TerailSee: 593-119 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f previously sent emails. In a son.win7@live.com f previously com f of the set of t	Ill of the emails, Ill of the emails, Ill of the emails, Ill of the emails	the Wescons predictore
FTTK found a to eiver was either peter End Atoms End Atoms	Index 32 Figure Figure Figure Figure tal of 15 en wilson.win ws Search Index Search Vol V	27 Texel: 27 e 39 Emai hails that 7 @ gmial tec 1	Highlighted: 0 Obscied: 0 still sent from peter were forwards or com or peterwill fill send forwards or fill send forwards or fill send forwards or fill send forwards	TextUser: 555410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f previously sent emails. In a son.win7@live.com f previously come texture	Ill of the emails, Ill of the emails, From The Accourt opterwise, mi78 Grad Accourt opterwis	the 2010 2
FTK found a to eiver was either peter Enal Res Enal Res E	Loaded: 27 Figure: Figure: Total of 15 en wilson.win wilson wilson win wilson win	27 Taxi: 27 e 39 Emails c 30 Emails c 30 Emails c 30 Emails c 425(20131) c	Hydrighted: 0 Checkled: 0 ail sent from pet were forwards or com or peterwill	TeallSee: 50x103 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com:	Ill of the emails,	المحمد المحم المحمد المحمد المحم المحمد المحمد ال المحمد المحمد ال
FTTK found a to eiver was either peter Enal Items Enal Items Enal Related Items (From Enal) (594/0) Enal Related Items (From Enal) (594	Index 32 Figure Figure tal of 15 en wilson.win vises idex Search Vol vises vise	27 Taxi: 27 e 39 Emails c 30 E	Hydrighted: 0 Checked: 0 ail sent from pet were forwards or com or peterwill 000000000000000000000000000000000000	TealLine: 503418 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com f previously sent emails. In a son.win7@live.com f previously sent emails. In a son.win7@live.com f previously and f the son of t	Ill of the emails,	۲ ۲ ۲ ۲
FTK found a to	Index Search (Video Searc	27 Text: 27 e 39 Ema hails that 7 @ gmial the 7 @ gmial th	Highlighted: 0 Obsided: 0 still sent from peter were forwards or .com or peterwill .iiii sent from peter .iiii sent from or peterwill .iiii sent from or peterwill .iiii sent from or peterwill .iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	TealSize 50410 erwilson.win7@live.com f previously sent emails. In a son.win7@live.com: typesty The Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Eastern Standard Time (from load machine) typesty Time Zone: Time Time Control T	Ill of the emails, Ill of the emails, Ill of the emails, Ill of the emails, Ill of the emails, th Ind Acourt operation with Gual Acourt	the where com- grad

Email Items 4 0	Fie List	_		a m rust	 Display Time Zope: Fast 	tern Standard Time (From Incal machine)	
Email Status					•	1-	· · · · · · · · · · · · · · · · · · ·
Email Attachments (0 / 0)	Name		Submit Time	Subject		10	From
Email Related Items (From Email) (584 / 0)	258A08D3-000	00014.eml	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email		"Gmail Account" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
- 🖓 Email Reply (18 / 18)	36DA6E6B-000	00017.eml	4/25/2013 10:30:21 P	Re: 04/25/2013 Daily Email		WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	peterwilson.win8@gmail.com
Forwarded Email (15 / 15)	00294823-000	00016.eml	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email		"Gmail Account" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
Email Archives	10226134-0000	00022.eml	5/1/2013 11:34:57 AM	Re: 05/01/2013 Daily Email v	with Text and Picture Attachments	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
E- Email by Date	10E66C58-000	00019.eml	4/25/2013 10:30:21 P	Re: 04/25/2013 Daily Email		WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	peterwilson.win8@gmail.com
- Call Email Addresses	2CD672AE-000	00027.eml	5/3/2013 4:49:04 PM (Re: 05/03/2013 Daily Email;		"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
+	7AA146F3-000	0001C.eml	4/26/2013 11:47:32 A	Re: 04/26/2013 Daily Email		"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	16496DF1-000	00011.eml	5/3/2013 4:49:04 PM (Re: 05/03/2013 Daily Email;		"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	18BE6784-0000	00006.eml	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email		"Gmail Account" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
	31751DDE-000	00008.eml	4/26/2013 11:47:32 A	Re: 04/26/2013 Daily Email		"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	48B31C64-000	00009.eml	4/25/2013 10:30:21 P	Re: 04/25/2013 Daily Email		WindowsSeven Forensics <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	peterwilson.win8@gmail.com
	26E901EB-0000	00009.eml	5/3/2013 4:49:04 PM (Re: 05/03/2013 Daily Email;		"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	20024E1C-000	00003.eml	4/26/2013 11:47:32 A	Re: 04/26/2013 Daily Email		"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	7998735E-0000	00006.eml	5/1/2013 11:34:57 AM	Re: 05/01/2013 Daily Email v	with Text and Picture Attachments	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	16496DF1-000	00014.eml	5/1/2013 11:34:57 AM	Re: 05/01/2013 Daily Email v	with Text and Picture Attachments	"Live Account" <peterwilson,win7@live.com></peterwilson,win7@live.com>	Gmail Account <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>
	2CD672AE-000	00010.eml	4/26/2013 11:47:32 A	Re: 04/26/2013 Daily Email		"Live Account" <peterwilson, win7@live.com=""></peterwilson,>	Gmail Account <pre>cpeterwilson.win7@gmail.com></pre>
	4AE13D6C-000	0001A.emi	5/3/2013 4:49:04 PM (Re: 05/03/2013 Daily Email:		"Live Account" <peterwilson, win7@live.com=""></peterwilson,>	Gmail Account <pre>cpeterwilson.win7@gmail.com></pre>
	00294823-0000	00003.eml	4/25/2013 10:07:32 P	Re: 04/25/2013 Daily Email		"Gmail Account" <peterwilson.win7@gmail.com></peterwilson.win7@gmail.com>	"Live Account" <peterwilson.win7@live.com></peterwilson.win7@live.com>
						1	

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:

05/01/2 Attachme From: Peter Wil To: "PeterWil Subject: 05/01/20 Sent: 05/01/20 Sent: Wed, 1 M Gent from PeterWilson.W Gent from PeterWilson.W Gent from Part, Type: Im Gent from Part, Type: Im Gen	D13 Daily Email with Text and Picture on speterwilson.win8@live.com> on.Win8@gmail.com" <peterwilson.win8@gmail.com>, WindowsSeven Forensics <peterwilson.win7@live.com>, ion.Win8@gmail.com" <peterwilson.win7@gmail.com>, WindowsSeven Forensics <peterwilson.win7@live.com>, ion.Win8@gmail.com" <peterwilson.win7@gmail.com>, is Daily Email with Text and Picture Attachments ay 2013 15:41:58 +0000 In8@live.com mge/jpeg; name="tiger_walking_rit_jpg", Disp: attachment; name="tiger_walking_rit_jpg", Size: 760KB] rge/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="o5012013attachment.txt", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 60 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp1442230bc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) cyeterwilson.win8@live.com> from bay0-omr1-s10.bay0.hotmail.com (bay0-omr1-s10.bay0.hotmail.com. [65.54.190.21]) by ms.google.com with</peterwilson.win7@gmail.com></peterwilson.win7@live.com></peterwilson.win7@gmail.com></peterwilson.win7@live.com></peterwilson.win8@gmail.com>	
rom: Peter Wil ro: "PeterWil Windows Subject: 05/01/20 Sent: Wed, 1 M ent from PeterWilson.W Mime Part, Type: im Mime Part, Type: im Mime Part, Type: im Mime Part, Type: te Delivered-To: Received: C-Received: C-Received: Receiv	on <pre>con <pre>con <pre>con <pre>con <pre>con <pre>con </pre> <pre>con.Win8@gmail.com? <pre>deterWilson.Win7@gmail.com>, WindowsSeven Forensics <peterwilson.win7@live.com>, ieven Forensics <peterwilson.win7@gmail.com> ia3 Daily Email with Text and Picture Attachments ay 2013 15:41:58 +0000 in8@live.com rge/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] rge/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] rt/plain; name="05012013attachment.txt", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id opmr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <pre>cypeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with </pre></peterwilson.win7@gmail.com></peterwilson.win7@live.com></pre></pre></pre></pre></pre></pre></pre>	
o: "PeterWil Windows aubject: 05/01/20 eent: 05/01/20 eent from PeterWilson.V Mime Part, Type: Im Mime Part,	on.Win8@gmail.com" <peterwilson.win8@gmail.com>, WindowsSeven Forensics <peterwilson.win7@live.com>, leven Forensics <peterwilson.win7@gmail.com> I3 Daily Email with Text and Picture Attachments ay 2013 15:41:58 +0000 in8@live.com inge/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] ige/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <peterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</peterwilson.win8@live.com></peterwilson.win7@gmail.com></peterwilson.win7@live.com></peterwilson.win8@gmail.com>	
Subject: 05/01/20 Sent: Wed, 1 M Sent from <u>PeterWilson.V</u> Mime Part, Type: im Mime Part, Type: im Mime Part, Type: te Delivered-To: Received: Received: Received: Received: Received: Received: Received: Received:	IS Daily Email with Text and Picture Attachments ay 2013 15:41:58 +0000 In8@live.com tige/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] tige/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="05012013attachment.txt", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) cyeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by ms.google.com with	
Sent: Wed, 1 M eent from <u>PeterWilson.V</u> Mime Part, Type: im Mime Part, Type: im Mime Part, Type: te Delivered-To: Received: C-Received: Received: Received: Received: Received: Received: Received:	ay 2013 15:41:58 +0000 in8@live.com age/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] age/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] at/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) cyeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mc.google.com with	
Sent from <u>PeterWilson.V</u> Mime Part, Type: im Mime Part, Type: im Mime Part, Type: te Delivered-To: teceived: teceived: teturn-Path: teceived: teceive: teceived: tecei	in&@live.com in&@live.com inge/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] inge/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <pre>cpeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</pre>	
ent from <u>PeterWilson.V</u> Mime Part, Type: im Mime Part, Type: im Mime Part, Type: te lecived-To: leceived:	<pre>in8@live.com ge/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] ge/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] d/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) cyeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</pre>	
Mime Part, Type: im Mime Part, Type: im Mime Part, Type: te belivered-To: teceived: Received: Received: teceived: teceived-SPF: Authentication-Result teceived:	<pre>ge/jpeg; name="tiger_walking_rit.jpg", Disp: attachment; name="tiger_walking_rit.jpg", Size: 760KB] ge/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) </pre>	
Mime Part, Type: im Mime Part, Type: te Delivered-To: Received: (-Received: R	<pre>ge/jpeg; name="tiger_walking_rit_color.jpg", Disp: attachment; name="tiger_walking_rit_color.jpg", Size: 625KB] t/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) cyeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</pre>	
Mime Part, Type: te Delivered-To: Received: (-Received: Received: Received: Received: Received-SPF: Nuthentication-Result	<pre>t/plain; name="05012013attachment.txt", Disp: attachment; name="05012013attachment.txt", Size: 80 bytes] peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <pterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</pterwilson.win8@live.com></pre>	
Delivered-To: Received: (-Received: Return-Path: Received: Received-SPF: Authentication-Result	peterwilson.win7@gmail.com by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <peterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</peterwilson.win8@live.com>	
Received: (-Received: Return-Path: Received: Received-SPF: Authentication-Result	by 10.182.223.6 with SMTP id qq6csp144223obc; Wed, 1 May 2013 08:46:28 -0700 (PDT) by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <peterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</peterwilson.win8@live.com>	
K-Received: Reteived: Received: Received-SPF: Authentication-Result	by 10.14.182.137 with SMTP id o9mr9569182eem.5.1367423187522; Wed, 01 May 2013 08:46:27 -0700 (PDT) <peterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with</peterwilson.win8@live.com>	
Return-Path: Received: Received-SPF: Authentication-Result	<pre><pre>cpeterwilson.win8@live.com> from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with </pre></pre>	
Received: Received-SPF: Authentication-Result	from bay0-omc1-s10.bay0.hotmail.com (bay0-omc1-s10.bay0.hotmail.com. [65.54.190.21]) by mx.google.com with	
Received-SPF: Authentication-Result	ESMTP id i8si3817639eem.207.2013.05.01.08.46.06 for <multiple recipients="">; Wed, 01 May 2013 08:46:27 -0700 (PDT)</multiple>	
Authentication-Result	pass (google.com: domain of peterwilson.win8@live.com designates 65.54.190.21 as permitted sender) client- ip=65.54.190.21;	
Pacaiwad:	:: mx.google.com; spf=pass (google.com: domain of peterwilson.win8@live.com designates 65.54.190.21 as permitted sender) smtp.mail=peterwilson.win8@live.com	
Received.	from BAY403-EAS16 ([65.54.190.60]) by bay0-omc1-s10.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675); Wed, 1 May 2013 08:43:50 -0700	
K-EIP:	[I1XQoEWphUTkJAZab55g4nNOWRwvrY+O]	
C-Originating-Email:	[peterwilson.win8@live.com]	
Message-ID:	<bay403-eas1613c75acfc7d4aad646beb3bc0@phx.gbl></bay403-eas1613c75acfc7d4aad646beb3bc0@phx.gbl>	
Return-Path:	peterwilson.win8@live.com	
MIME-Version:	1.0	
mportance:	Normal	
Content-Type:		

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 Registry 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\OpenSavePIDIMRU we are able to see a listing of files that have recently been opened

Name	Туре	Data
8 MRUListEx	REG_BINARY	07 00 00 00 06 00 00 00 05 00 00 00 04 00 00 03 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
B 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 01 A 00 EE BB FE 23 00 00 10 00 7D B1 0D 7B D2 9C 93 4A 97 33 46 CC 89 02
20 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
B 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
80 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
883	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
BE 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
殿 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 OpenSavePIDIMRU 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 ? SD . AU 10 FE 6B 30 EE 20 00 00 00-1A 00 EE BB FE 23 00 00 pk01 ·····1»p#· ···âM7? ·eE ·d9Å ·^ 20 10 00 90 E2 4D 37 3F 12-65 45 91 64 39 C4 92 5E 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 ····14····*· 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:

Name	Туре	Data
nruListEx	REG_BINARY	03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
111 3	REG_BINARY	77 00 6C 00 6D 00 61 00 69 00 6C 00 2E 00 65 00 78 00 65 00 00 00 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
<u>80</u> 2	REG_BINARY	69 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 2E 00 65 00 78 00 65 00 00 00 14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 0
興 1	REG_BINARY	6E 00 6F 00 74 00 65 00 70 00 61 00 64 00 2E 00 65 00 78 00 65 00 00 00 14 00 1F 42 25 48 1E 03 94 7B C3 4D B1 31 E9 46 B4 4C 8D D5 74 00 00 00 1
BU 0	REG_BINARY	66 00 69 00 72 00 65 00 66 00 6F 00 78 00 2E 00 65 00 78 00 65 00 00 00 14 00 1F 44 47 1A 03 59 72 3F A7 44 89 C5 55 95 FE 6B 30 EE 20 00 00 00 1

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	Туре	Data	00.00.00.00.00			11.00.00	00.10.00	00.00.02		0.05.04		4 00 00 00 05 00 00 00 00 00 00 00 00	
	11 5	REG_BINARY	30.00.35.00	30.00.34.00.3	0.00.31.0	0 03 00 00 00 1 0 33 00 64 00 6	51 00 00	00 10 00	79 00 28	00 00 0	0 0F 00	0 74 00 2	4 00 00 00 02 00 00 00 00 00 00 00 00 00	2 00 00 00 08
	i i i i i i i i i i i i i i i i i i i	REG_BINARY	30 00 35 00	30 00 33 00 3	2 00 30 0	0 31 00 33 00 6	64 00 65	00 6C 00	65 00 74	4 00 65 0	0 64 0	0 2E 00 7	4 00 78 00 74 00 2E 00 74 00 78 00 74	4 00 00 00 82
	11	REG_BINARY	30 00 35 00	30 00 33 00 3	2 00 30 0	0 31 00 33 00 6	61 00 74	00 74 00	61 00 63	8 00 68 0	0 6D 0	0 65 00 6	E 00 74 00 2E 00 74 00 78 00 74 00 2E	00 74 00 78
	<u>3</u> 3	REG_BINARY	30 00 35 00	0 30 00 33 00 3	2 00 30 0	0 31 00 33 00 6	64 00 61	00 69 00	6C 00 79	9 00 2E 0	0 74 0	0 78 00 7	4 00 2E 00 74 00 78 00 74 00 00 00 70	00 32 00 00
	17	REG_BINARY	30 00 35 00	30 00 32 00 3	2 00 30 0	0 31 00 33 00 6	64 00 61	00 69 00	6C 00 79	9 00 2E 0	0 74 0	0 78 00 7	4 00 2E 00 74 00 78 00 74 00 00 00 70	00 32 00 00
	16 80 2	REG_BINARY	30 00 35 00) 30 00 31 00 3	2 00 30 0	0 31 00 33 00 6	64 00 65 61 00 74	00 6C 00	65 00 74 61 00 63	100650	0.64.0	0 2E 00 7 0 65 00 6	4 00 78 00 74 00 2E 00 74 00 78 00 74 5 00 74 00 2E 00 74 00 78 00 74 00 25	1 00 00 00 82
	15 L	REG_BINARY	30.00.35.00	30 00 31 00 3 1 30 00 31 00 3	2 00 30 0 2 00 30 0	0.31.00.33.007	64 00 61	00 69 00	6C 00 79	9 00 00 0 9 00 2F 0	0 82 0	0 85 00 8 0 78 00 7	2 00 74 00 22 00 74 00 78 00 74 00 00 22 4 00 2F 00 74 00 78 00 74 00 00 00 70	00 32 00 00
	11 4	REG BINARY	44 00 6F 00) 77 00 6E 00 6	C 00 6F 0	0 61 00 64 00 3	73 00 00	00 64 00	32 00 0	0000000	0 00 0	0 00 00 0	0 00 44 6F 77 6E 6C 6F 61 64 73 2E 6	C 6E 6B 00 4
	14	REG_BINARY	72 00 69 00	74 00 SF 00 6	1 00 6C 0	0 75 00 6D 00	5F 00 61	00 73 00	73 00 6	F 00 63 0	0 2E 0	0 6A 00 7	70 00 67 00 00 00 74 00 32 00 00 00 0	0 00 00 00 0
	BE 13	REG_BINARY	74 00 69 00	67 00 65 00 7	2 00 5F 0	0 77 00 61 00 6	6C 00 68	00 69 00	6E 00 67	7 00 5F 0	0 72 0	0 69 00 7	4 00 5F 00 63 00 6F 00 6C 00 6F 00 72	2 00 2E 00 6
	12	REG_BINARY	74 00 69 00	67 00 65 00 7	2 00 5F 0	0 77 00 61 00 6	6C 00 68	00 69 00	6E 00 67	7 00 5F 0	0 72 0	0 69 00 7	4 00 2E 00 6A 00 70 00 67 00 00 00 7	C 00 32 00 0
	11 11	REG_BINARY	72 00 69 00	74 00 5F 00 7	7 00 68 0	0 69 00 74 00 6	65 00 SF	00 6E 00	6F 00 5F	00 62 0	0 61 00	0 72 00 2	E 00 6A 00 70 00 67 00 00 00 7A 00 3	2 00 00 00 00
	10 80 o	REG_BINARY	72 00 69 00) /4 UU 5F UU 6) 32 00 38 00 3	200600	0 51 00 53 00 0	68 00 5F 64 00 65	00.65.00	6F 00 5/	- UU 62 U 1 00 65 0	0 64 0	0 72 00 2	12 00 6A 00 70 00 67 00 00 00 7A 00 3 14 00 78 00 74 00 2E 00 74 00 78 00 74	2 00 00 00 0
	1 8	REG_BINARY	30 00 34 00) 32 00 38 00 3	2 00 30 0	0 31 00 33 00 6	64 00 61	00 69 00	6C 00 79	9 00 2E 0	0 74 0	0 78 00 7	4 00 2E 00 74 00 78 00 74 00 00 00 70	00 32 00 00
	1 7	REG_BINARY	44 00 6F 00	63 00 75 00 6	D 00 65 0	0 6E 00 74 00	73 00 00	00 64 00	32 00 00	0 00 00 0	0 00 0	0 00 00 0	0 00 44 6F 63 75 6D 65 6E 74 73 2E 6	C 6E 6B 00 4
				Fi	gure	47 Rece	entD	ocs R	legis	try I	Key			
As w	as the case	e with the p	previous	registry	key,	the data	a por	tion a	ppea	ars in	hey	xadeo	cimal but Registry V	iewer can
conve	ert that into	o ASCII te	xt:											
												0 F		
		00 3	30 00 35	00 30	JU 33	00-32 0	00 3	J UU ;	31 0	0 33	00	0.5.	0.3.2.0.1.3.	
		10 6	54 00 65	00 60	0 65	00-74 0	00 6	5 00 1	54 0	J ZE	00	d·e·	l·e·t·e·d·.·	
		20 7	4 00 78	00 74	JU 28	00-74	00 7		74 0	000	25	t·x·	tt.x.t	
		40 3	20 33 32	30 31	33 64	65-60	65 7	1 65 1	54 21	2 24	20	0320	12deleted ty	
		40 3	00 JJ JG 00 JD GC	30 31 . CP CD	33 64 30 60	00-00 0	00 0	4 00 1	04 41 77 D1	2 00	20	0.320. + 1ml	Louistered. CX	
		50 /	14 26 60	00 00	JU 30 10 20	00-00			5F DI	00 0	00	c.m	к.,ты	
		70 0	0 00 00	00 00 0	00 28	00-00				0 00	00			
		80 3	30 00 35	00 30	10 33	00-32 0	00 3		31 0	1 33	00	0.5.	0.3.2.0.1.3.	
		90.6	54 00 65	00 60	10 65	00-74	00 6	5 00 0	54 DI	1 2E	00	d-e-	leted	
		a0 7	74 00 78	00 74	00 2E	00-60	00 61	E 00 3	5B 00	0 00	00	t·x·	tl.n.k	
		b0 2	26 00 00	00								6 · · ·		
		Figure 4	48 HEX	and AS	SCII	Data R	EG_	BINA	ARY	0 R	ecei	ntDo	cs Registry Key	
From	this wa co	on soo that	the follo	wing ne	mag	correspo	and t	o tha	folle	win	n 91	nlica	tions	
TIOII	i uns we ca		the fond	owing in	unes	concept	Jilu (0 the	TOIL) w III g	g ap	prica	utons.	
				Т	able	13 Rece	entD	ocs A	ppli	catio	ons			
				Nam	e	A	Appl	icatio	n in	Tex	t]	
				15		0501	201	3attac	hme	nt.tx	t.lnl	k		
				14		Ι	Rit_a	lum_	asso	c.lnk	2			
				13		Tiger	r_wa	lking	_rit_	colo	r.lnl	k		
				12			Tige	r_wal	lking	g.lnk				
				11		R	it_w	hite_1	no_b	ar.ln	k			
				10		R	it_bl	ack_1	10_b	ar.ln	k			
				9		042	2820	13del	leted	.txt.l	nk			
				8		04	4282	013da	aily.1	txt.ln	k			
				7			Do	cume	nts.l	nk				
				5		05	5032	013da	aily.t	xt.ln	k			
				4			Do	wnblo	oads.	lnk				
				3		05	5032	013da	aily.1	xt.ln	k			

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	Туре	Data
Bias	REG_DWORD	0x0000012C (300)
醚DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
ab]DaylightName	REG_SZ	@tzres.dll,-111
鍵 DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
鼷StandardBias	REG_DWORD	0×00000000 (0)
ab)StandardName	REG_SZ	@tzres.dll,-112
鼷 StandardStart	REG_BINARY	00 00 08 00 01 00 02 00 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
B DynamicDaylightTimeDisabled	REG_DWORD	0×00000000 (0)
B ActiveTimeBias	REG_DWORD	0×000000F0 (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	Туре	Data
	REG_SZ	{7A31582A-B896-4519-B9C6-463F6BB258FD}
ab Description	REG_SZ	Network 2
選 Source	REG_DWORD	0×00000008 (8)
a DnsSuffix	REG_SZ	localdomain
FirstNetwork	REG_SZ	Network 2
Contraction (Contraction of the second secon	REG_BINARY	00 50 56 F2 6C 68
1		

Figure 50 Unmanaged Network 2 Registry Key

Name	Туре	Data
and ProfileGuid	REG_SZ	{2456B97F-7C61-44A6-A66C-DCAC8AFB6820}
Description	REG_SZ	Network
🥰 Source	REG_DWORD	0×00000008 (8)
and Dissuffix	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:

Ξ	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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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 [NTF5]/[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

Hex	Т	ext	Filt	ered	I N	atur	al									
00	54	68	69	73	20	66	69	6C-65	20	77	61	73	20	63	72	This file was cr
10	65	61	74	65	64	20	6F	6E-20	30	35	2F	30	33	2F	32	eated on 05/03/2
20	30	31	33	20	61	74	20	34-3A	35	38	50	4D				013 at 4:58PM

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	Accessed	Created	Written	Analysis	Type	Path
\$RFGBREV.txt	83	04/28/13 04:31:08 PM	04/28/13 04:08:13PM	04/28/13 04:08:13PM	Match	Text	Windows 8-flat\C\Recovered Folders\.\\$Recycle.Bin\S-1-5-21-1414118115-6188285350-1081150
🚦 \$IFGBRE V.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-1-5-21-1414118115-6188285350-1081150
The	first	file, \$RFC	Figu GBREV.txt	tre 56 Wit	ndow: ollowi	s 8 Recovered	d Deleted Files
Fields 🐻 Rej	port 🛅	Text 🔠 Hex 🛗 D	ecode 📧 Doc 📰 1	Transcript 📲 Picture		-	Lock
Options 🍡 C	odepage ·	🔹 🗛 Text Style 👻 🎢	Find 🔄 🛅 📜 🛛	Compressed View	🕈 Previous	Item 🛄 Next Item	
68 69 73 2	20 66 69	6C 65 20 77 61 7	3 20 63 72 65 61 5 20 77 61 73 20	74 65 64 20 6F 6E 64 65 6C 65 74 65	20 30 34 64 20 6F	2F 32 38 2F 32 30 31 3 6E 20 30 34 2F 32 38 2	3 20 61 74 20 34 3A 31 30 F 32 30 31 33 20 61 74 PM This file was deleted on 04/28/2013 at 4:10
50 4D OD OA 3	54 68 69	73 20 00 07 00 0	T:	auno 57 D	0001	and File ¢DL	
The	seco	nd file, \$I	Fi FGBREV.	gure 57 R txt has the	ecovo follo [,]	ered File \$RF wing contents	GBREV.txt
The	54 68 69 SECO port 🖭	nd file, \$∏	Fi FGBREV. ∝ode ≝Doc ≧1	gure 57 R txt has the	ecov follo	ered File \$RH wing contents	GBREV.txt :
The Fields Re Options "A C	SECO	nd file, \$I	Fi FGBREV. ecode © Doc 🗊	gure 57 R txt has the ranscript Picture	ecovo follo ^s	ered File \$RF wing contents Rem NextRem	GBREV.txt : . lock c

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	Uri 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=AQLbntWvThXn1fWGqxujzCfLzoPq86sXDCAP1m6AYWUEeXZ	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_nWl3I	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_vThe_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_kITrH2DsgfsQE4Zy8z2htuiKkqUGJ9oI	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	Uri Name	Internet Artifact Typ
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	Uri 🔺 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	'Uri 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-IVb_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:

- Internet	·		Piere u	2	
Internet F	volorer (Mindows)	🔠 Table 🥹 Timeline	E Gallery		
A D Chrome IV	Vindows)	🎲 🏢 👻 🚖 🖵 🔲 Sele	cted 0/3318		
Cookie	s	Browser	Url	Internet	Created
- Dain E)ata	Туре	Name	Artifact Type	
-D- Top Site	es	1 Chrome (Windows)	https://twitter.com/	Login Data	04/21/13 04:49:59PM
Downlo	pads	2 Chrome (Windows)	https://www.facebook.com/	Login Data	04/21/13 04:49:35PM
-D- History					
🖌 🕞 🚺 Cache					
-Dial Imag	je				
-D- Unki	nown Type				
-D-D- Code	e				
—⊳ нтм	L				
-D-D- Font	is and the second se				
-D-D- Vide	0				
🕨 🕞 📗 Mozilla (M	/indows/Mac)				
🕞 🖂 🌗 Mozilla 3 ((Windows/Mac)				
* Zoom In * Zoor	n Out 🐟 100% 👻 [👕 Previous Item 🗋 Next I	tem		
Zoom In Zoor Internet Artifact Type	n Out 🔍 100% 👻 🗌 Login Data	👚 Previous Item [🗋 Next I	tem		
♥ Zoom In ♥ Zoor Internet Artifact Type Url Name	n Out	👚 Previous Item 🛛 🗋 Next I	tem		
Zoom In Zoor Internet Artifact Type Url Name Url Host	n Out	next I The second secon	tem		
Zoom In Zoor Internet Artifact Type Url Name Url Host Action Url	n Out	Previous Item Next I bok.com/	tem		
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username	n Out 😍 100% 👻 Login Data https://www.facebo www.facebook.com, https://www.facebo email	Previous Item Next I book.com/	tem		
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element Usern	n Out 😍 100% 👻 Login Data https://www.facebo www.facebook.com, https://www.facebo email	Previous Item Next I book.com/ / hook.com/login.php	tem		
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element User Dascuper Element	n Out 😍 100% 👻 Login Data https://www.facebo www.facebook.com, https://www.facebo email peterwilson.win8@	T Previous Item 💽 Next I)ook.com/ / ook.com/login.php gmail.com	tem		
Zoom In Zoom Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element Pascword Value	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebook.com, https://www.facebook.com, email peterwilson.win8@ pass of on on on do scad	Previous Item Next I bok.com/ / wok.com/login.php gmail.com	tem	18 bd 09 8c 4c	b1 53
Zoom In Zoom Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element Password Value	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebook.com, https://www.faceboo email peterwilson.win8@ pass 01 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00	Previous Item Next I vok.com/ / / pok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 02 00 00 00 00 01	tem * -2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 01 00 00 20 00 00	18 bd 09 8c 4c 1 00 e5 9b ab 1	b1 53 9 31
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebo	Previous Item Next I vok.com/ / / pok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 00 20 00 00 00 00 11 3f 63 34 a5 3c 0e 01 85 11 29	tem - c2 97 eb 01 00 00 00 f4 fd df 4 - 66 00 00 00 01 00 00 20 00 00 46 3c 5b d1 25 05 0e 94 01 77	18 bd 09 8c 4c 1 00 e5 9b ab 1 00 00 00 00 0e	b1 53 9 31 80_
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebo	Previous Item Next I bok.com/ / bok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 00 00 00 00 00 00 00 1 3f 63 34 a5 3c 0e 01 85 11 29 00 00 00 91 eb fd bf 50 bd 3 se c5 10 00 00 00 00 00 ft 9 31 98	tem 2 2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 01 00 00 20 00 00 46 3 5 b d1 25 05 0e 94 01 77 b d1 a9 57 19 fb 63 0b cb b2 4 0 82 12 26 5 cb 27 6 d2 b 4 0	18 bd 09 8c4c 00 e5 9b ab 1 00 00 00 00 00 1 9c b2 fb 2e fc 20 ce 40 00 00	b1 53 9 31 80 4 37
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value	n Out 😍 100% 🗸 Login Data https://www.facebook.com, https://www.facebook.com, https://www.faceboo email peterwilson.win8@ pass 01 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c 18 01 f6 b9 17 8 00 00 00 02 00 00 20 16 25 8 fb 64 96 53 5	Previous Item Next I bok.com/ / wok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 02 00 00 00 00 00 01 f63 34 a5 3c 00 11 85 11 29 00 00 00 91 eb fd bf 50 bd 3 e8 c5 10 00 00 00 cf 1b 31 9f 46 ef 7 a1 66 05 72 1f e7 ac	tem - c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 46 3 c5 b 12 50 50 e9 40 1 77 b d1 a9 57 19 fb 63 0b cb b2 4 9 83 12 26 95 cb 27 6d 2b 49 cl ce 0f 0b 64 f8 12 75 59 bb 7e:	18 bd 09 8c4c1 00 e5 9b ab 1 00 00 00 00 1 9c b2 fb 2e fr .70 ce 40 00 00 3a 67 37 4c6b	b1 53 9 31 80 4 37 000 fd cf
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebook.com, https://www.facebook.com, https://www.faceboo email peterwilson.win8@ pass 01 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c 18 01 f6 b9 17 8 00 00 00 02 00 00 20 1 80 d6 b8 e0 6e 02 0c 1f 25 e3 fb a4 96 53 5 bf 6c d5 55 22 eb ad	Previous Item Next I bok.com/ / yok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 02 00 00 00 00 00 01 8f 63 34 a5 3c 0e 01 85 11 29 00 00 00 91 eb fd bf 50 bd 3 e8 c5 10 00 00 00 cf 1b 31 9g 46 6e f7 a1 c6 05 72 1f e7 ac d8 0e 75 22 48 96 31 54 cd 55	tem - c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 46 3c 5b d1 25 05 0e 94 01 77 b d1 a9 57 19 fb 63 0b cb b2 4 0 83 12 26 95 cb 27 6d 2b 49 cd ce 0f 0b 64 f8 12 75 59 bb 7e : ce 32 0e 81 de 65 ee 3e c4 6f 1	18 bd 09 8c 4c 00 e5 9b ab 1 00 00 00 00 00 26 19 c b2 fb 2e fr .70 ce 40 00 00 3a 67 37 4c 6b f 93 97 de	b1 53 9 31 80 4 37 0 00 fd cf
Zoom In Zoom Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element Password Value Signon Realm	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebook.com, https://www.faceboo email peterwilson.win8@ pass 01 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c 18 01 f6 59 17 8 00 00 00 00 20 00 20 0 80 d6 b8 e0 6e 02 0c 1f 25 e3 fb a4 96 53 5 b f6c d5 55 22 eb ad https://www.facebo	Previous Item Next I bok.com/ / yok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4t 00 00 00 02 00 00 00 00 01 13f 63 34 a5 3c 0e 01 85 11 29 00 00 00 91 eb fd bf 50 bd 3 e8 c5 10 00 00 00 cf 1b 31 95 54 6e f7 a1 c6 05 72 1f e7 ac d8 0e 75 22 48 96 31 54 cd 5 bok.com/	tem - c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 46 3c5 b d1 25 05 0e 94 01 77 b d1 a9 57 19 fb 63 0b cb b2 4 9 83 12 26 95 cb 27 6d 2b 49 cl ce 0f 0b 64 f6 12 75 59 bb 7e : ic a2 0e 81 de 65 ee 3e c4 6f 1	18 bd 09 8c 4c 100 e5 9b ab 1 00 00 00 00 00 0e 1 9c b2 fb 2e fr . 70 ce 40 00 00 3a 67 37 4c 6b .f 93 97 de	b1 53 9 31 80 4 37 0 00 fd cf
Zoom In Zoom Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element Password Value Signon Realm Ssl Valid	n Out 😍 100% - Login Data https://www.facebook.com, https://www.facebook.com, https://www.facebook.com, https://www.faceboo email peterwilson.win8@ pass 01 00 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c 18 01 f6 b9 17 8 00 00 00 00 00 00 00 20 80 d6 b8 e0 6e 02 0c 1f 25 e3 fb a4 96 53 3 bf 6c d5 55 22 eb ad https://www.faceboo 1	Previous Item Next I vok.com/ / / pok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 02 00 00 00 00 01 3f 63 34 a5 3c 0e 01 85 11 29 3f 63 54 a5 3c 0e 01 85 11 29 54 6e f7 a1 c6 05 72 1f e7 ac d8 0e 75 22 48 96 31 54 cd 9 pok.com/	tem ¹ c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 46 3c5 b d1 25 05 0e 94 01 77 b d1 a9 57 19 fb 63 0b cb b2 4: 0 83 12 26 95 cb 27 6d 2b 49 d ce 0f 0b 64 f8 12 75 59 bb 7e : ¹ ca 2 0e 81 de 65 ee 3e c4 6f 1	18 bd 09 8c 4c 1 00 e5 9b ab 1 00 00 00 00 00 1 9c b2 fb 2e f4 70 ce 40 00 00 3a 67 37 4c 6b f 93 97 de	b1 53 9 31 80 4 37 000 fd cf
Zoom In Zoom Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value Signon Realm Ssl Valid Preferred cont	n Out 😍 100% 👻 Login Data https://www.facebook.com, https://www.facebook.com, https://www.facebooken email peterwilson.win8@ pass 01 00 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c 18 01 f6 b9 17 8 00 00 00 00 00 00 20 01 125 e3 fb a4 96 53 3 bf 6c d5 55 22 eb ad https://www.facebool 1 1	Previous Item Next I vok.com/ yok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 00 00 00 00 00 00 11 sf 63 34 a5 3c 0e 01 85 11 29 00 00 00 01 eb fd bf 50 bd 31 95 S4 6e f7 a1 d6 05 72 1f e7 ac d8 0e 75 22 48 96 31 54 cd 5 yok.com/	tem (c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 46 3c5b d1 25 05 0e 94 01 77 b d1 a9 57 19 fb 63 0b cb b2 43 98 12 26 95 cb 27 6d 2b 49 d ce 0f 0b 64 f8 12 75 59 bb 7e 1 (c a2 0e 81 de 65 ee 3e c4 6f 1	18 bd 09 8c 4c 1 00 e5 9b ab 1 00 00 00 00 00 1 9c b2 fb 2e f 7 0 ce 40 00 00 3a 67 37 4c 6b f 93 97 de	b1 53 9 31 :80 4 37 000 fd cf
Zoom In Zoom In Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value Signon Realm Ssl Valid Preferred Created	n Out 😍 100% - Login Data https://www.facebook.com, https://www.facebook.com, https://www.facebook.com, https://www.faceboo pass 01 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c18 01 f6 b9 17 8 00 00 00 02 00 00 20 1 80 d6 b8 e0 6e 02 0c 11 25 e3 fb a4 96 53 5 bf 6c d5 55 22 eb ad https://www.faceboo 1 04/21/13 04:49:35PM	Previous Item Next I bok.com/ / wok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 4f 00 00 00 02 00 00 00 00 00 01 f63 34 a5 3c0 e01 85 11 29 000 00 09 1 eb fd bf 50 bd 3 e8 c5 10 00 00 07 1b 31 9f 36 6e f7 a1 dc 60 57 2f fe7 ac d8 0e 75 22 48 96 31 54 cd 9 wok.com/	tem 1 c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 46 3 c5 b 12 50 50 e9 40 1 77 b d1 a9 57 19 fb 63 0b cb b2 4 0 83 12 26 95 cb 27 6d 2b 49 cl ce 07 0b 64 f8 12 75 59 bb 7 e: 1 c a2 0e 81 de 65 ee 3e c4 6f 1	18 bd 09 8c4c1 00 e5 9b ab 1 00 00 00 00 1 9c b2 fb 2e fr .70 ce 40 00 00 3a 67 37 4c6b f 93 97 de	b1 53 9 31 80 4 37 0 00 fd cf
 Zoom In Zoor Internet Artifact Type Uri Name Uri Host Action Uri Usermame Element User Password Element Password Value Signon Realm Ssi Valid Preferred Created Blacklisted 	n Out € 100% ▼ Login Data https://www.facebook.com, https://www.facebook.com, https://www.facebook.com, https://www.faceboo email peterwilson.win8@ pass 01 00 00 00 d0 8c 9d d5 95 f4 37 db e4 00 36 3c 18 01 f6 99 17 6 00 00 00 02 00 00 20 1 80 d6 b8 e0 6e 02 0c 1f 25 e3 fb a4 96 53 5 5f 6c d5 55 22 eb ad https://www.faceboo 1 04/21/13 04:49:35PM 0	Previous Item Next I bok.com/ / yok.com/login.php gmail.com df 01 15 d1 11 8c 7a 00 d0 44 00 00 00 02 00 00 00 00 00 01 87 63 34 a5 3c 0e 01 85 11 29 00 00 00 91 eb fd bf 50 bd 3 e8 c5 10 00 00 00 cf 1b 31 99 46 ef 7a 1d 60 57 21 fe 7 ac d8 0e 75 22 48 96 31 54 cd 5 yok.com/	tem - c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 01 00 00 20 00 00 46 3c 5b d1 25 05 0e 94 01 77 b d1 a9 57 19 fb 63 0b cb b2 4 9 83 12 26 95 cb 27 6d 2b 49 cd ce 0f 0b 64 f8 12 75 59 bb 7e i c a2 0e 81 de 65 ee 3e c4 6f 1	18 bd 09 8c4c 00 e5 9b ab 1 00 00 00 00 00 26 19 c b2 fb 2e fr .70 ce 40 00 00 3a 67 37 4c6b f 93 97 de	b1 53 9 31 80 4 37 0 00 fd cf

	nternet) 🔻 🛄 Split I	Mode - SE Condition -	🍿 Filter 👻 🗢 Tags 👻 🖾 F	Review Packad	e 🔻 \infty Bookmark 💌
D		Table M Timeline	E Gallery		
DInternet E	xplorer (Windows)		- concil		
- DI Chrome (V	Vindows)	💵 ▼ 🔁 ↓ ▼ 🛄 Sele	ected 0/3318		
-D- Cookie	s	Browser	Url	Internet	Created
— 🕒 📔 Login 🛙)ata	Type	Name	Artifact Type	04/04/40 04:40 50514
-D-D Top Site	es	I Chrome (Windows)	https://twitter.com/	Login Data	04/21/13 04:49:59PM
-D-D Downlo	bads	2 Chrome (Windows)	https://www.facebook.com/	Login Data	04/21/13 04:49:35PM
-D-D- History					
🔺 🖓 🛄 📔 Cache					
-D- 📗 Imag	je				
-D- 🛄 Unki	nown Type				
-D- Cod	e				
——————————————————————————————————————	L				
-D-D- Font	ts				
🗆 🖂 📗 Vide	0				
🕨 🕞 🚺 Mozilla (M	/indows/Mac)				
🕨 🕞 🚺 🕹 🕹 🕹	(Windows/Mac)				
🕈 Zoom In 🛛 🗖 Zoor	n Out 🔍 100% 🔻	📑 Previous Item 📑 Next	Item		
Internet Artifact	Login Data				
Internet Artifact Type Ud Name	Login Data	~/			
Internet Artifact Type Url Name Url Host	Login Data https://twitter.com	n/			
Internet Artifact Type Url Name Url Host Artion Url	Login Data https://twitter.com twitter.com/ https://twitter.com	n/			
Internet Artifact Type Url Name Url Host Action Url Username	Login Data https://twitter.com twitter.com/ https://twitter.com session/username	n/ n/sessions = or email1			
Internet Artifact Type Url Name Url Host Action Url Username Element	Login Data https://twitter.com twitter.com/ https://twitter.com session[username	n/ n/sessions e_or_email]			
Internet Artifact Type Url Name Url Host Action Url Username Element User	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@	n/ n/sessions e_or_email] @live.com			
Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password	n/ n/sessions e_or_email] @live.com 1]			
Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element Password Value	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 d0 8c 9c d5 95 f4 37 db e4 00 f1 dc f9 1a 81 9b cb	n/ =_or_email] @live.com t] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 02 00 00 00 00 01 5e ac e8 5a 9c cf 72 6f 32 fd	f c2 97 eb 01 00 00 00 f4 fd df .0 66 00 00 00 01 00 00 20 00 00 3c c8 1a 1c bf fd 73 01 81 85 0	48 bd 09 8c 4c 0 00 fd 5c 5a 4d 0 00 00 0e 8	b1 53 :71 0 00
Internet Artifact Type Url Name Action Url Username Element User Password Element Password Value	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 d0 8c 9c d5 95 14 37 db e4 00 f1 dc 19 1 81 9b cb 00 00 02 00 00 20 00	n/ n/sessions e_or_email] @live.com i] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 20 c0 00 00 00 00 00 5 E a c e 8 5a 9c cf 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d	f <2 97 eb 01 00 00 00 f4 fd df .0 66 00 00 00 10 00 00 00 00 3c <8 1 a 1 c bf fd 73 01 81 85 00 60 4f 72 fa 7c 91 4a e7 6f 0e bf	48 bd 09 8c 4c 100 fd 5c 5a 4c 0 00 00 00 8c 1 ff d8 a0 36 37	b1 53 ;71 0 00 fd
Internet Artifact Type Url Name Action Url Username Element User Password Element Password Value	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 00 80 90 d5 95 f4 37 db e4 00 f1 dc f9 1a 81 9b cb 00 00 02 00 00 20 00 89 ee 7a 7f d6 07 f2 09 8b cc d6 68 50 32	n/ e_or_email] @live.com i] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 02 00 00 00 00 0 5 5a ec e8 5a 9c d7 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d i 2 96 10 00 00 0d f34 76 d6 ff 4 e2 1a cc 87 5d 38 59 2d d1	f c2 97 eb 01 00 00 00 f4 fd df4 0 66 00 00 00 00 100 00 20 00 00 3c c8 1a 1c bf fd 73 01 81 85 00 60 4f 72 fa 7c 91 4a e7 6f 0e bf 77 bd 07 96 99 2c 9f 05 cb 7c fr 25 64 7d 0a 8e f5 09 55 4f 4d a	48 bd 09 8c 4c 0 00 fd 5c 5a 4 0 00 00 00 8 iff d8 a0 36 37 6 40 00 00 00 00	b1 53 71 000 fd 9 e6 19 5f
Internet Artifact Type Url Name Artion Url Username Element User Password Element Password Value	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 d0 8c 9d d5 95 F4 37 db e4 00 f1 dc f9 1a 81 9b cb 00 00 02 00 00 20 00 89 ee 7a 7f d6 07 f2 09 8b ce d4 68 50 84 92 51 55 Ie 3a 16 66	n/ e_or_email] @live.com i] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 02 00 00 00 00 0 5 5a ac e8 5a 9c df 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d 0 00 00 9c ba 49 18 ee d8 7d d1 d fe b6 61 d0 13 cb be 42 09 5	f <2 97 eb 01 00 00 00 f4 fd df 4 .0 66 00 00 00 01 00 00 20 00 00 3c d8 1a 1c bf fd 73 01 81 85 00 50 4f 72 fa 7c 91 4a e7 6f 0e bf 77 bd 07 96 99 2c 9f 05 cb 7c fi 25 64 7d 0a 8e f5 09 55 4f 4d a 5a 43 79 a2 91 4b a7 9b 4d 0d 3	48 bd 09 8c 4c 00 fd 5c 5a 40 00 00 00 00 0e 8 * ff d8 a0 36 37 6 40 00 00 00 e d 92 02 e6 86 9c1e 9a	b1 53 :71 0 00 fd 9 e6 d9 5f
Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 d0 80 9d d5 95 f4 37 db e4 00 f1 dc f9 1a 81 9b cb 00 00 02 00 00 20 00 89 ee 7a 7f d6 07 f2 99 8b ce d4 68 50 84 92 51 55 1e 3a 16 6d https://twitter.com	n/ se_or_email] @live.com 1] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 02 00 00 00 00 00 1 5 5e ac e8 5a 9c df 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d 1 2 96 10 00 00 00 df 34 76 d6 ff 4 e2 1a cc 87 5d 38 59 2d d1 d fe b6 61 d0 13 cb be 42 09 9 n/	f c2 97 eb 01 00 00 00 f4 fd df4 .0 66 00 00 00 01 00 00 20 00 00 3 c 63 la 1 c bf fd 73 01 81 85 01 60 4f 72 fa 7 c 91 4a e7 6f 0e bf 77 bd 07 96 99 2 c 9f 05 cb 7 c fi 25 64 7d 0a 8e f5 09 55 4f 4d a 5a 43 79 a2 91 4b a7 9b 4d 0d 5	48 bd 09 8c 4c 0 00 fd 5c 5a 4c 0 00 00 00 00 36 37 6 40 00 00 00 e d 92 02 e6 86 c 9c 1e 9a	b1 53 :71 0 00 fd 9 e6 19 Sf
Internet Artifact Type Uri Name Uri Host Action Uri Usermane Element User Password Element Password Value	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 00 08 c9c d5 95 f4 37 db e4 00 f1 dc f9 1a 81 9b cb 00 00 02 00 00 20 00 89 ee 7a 7f d6 07 f2 09 8b ce d4 68 50 84 92 51 55 1e 3a 16 6c https://twitter.com 1	n/ e_or_email] @live.com f] d df 01 15 d1 11 8c7a 00 d0 4 0 00 00 00 02 00 00 00 00 00 0 5 5e ac e8 5a 9c cf 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d 2 96 10 00 00 00 df 43 76 ds ff 4 e2 1a cc 87 5d 38 59 2d d1 d fe b6 61 d0 13 cb be 42 09 9 n/	f c2 97 eb 01 00 00 00 f4 fd df 4 .0 66 00 00 00 01 00 00 20 00 00 3c c8 1 a 1 c bf fd 73 01 81 85 0 60 4f 72 fa 7c 91 4a e7 6f 0e bf 77 bd 07 96 99 2c 97 65 cb 7c f 25 64 7d 0a 8e f5 09 55 4f 4d a 5a 43 79 a2 91 4b a7 9b 4d 0d 5	48 bd 09 8c 4c 0 00 fd 5c 5a 4d 0 00 00 00 0e 8 * ff d8 a0 36 37 6 40 00 00 00 d 92 02 e6 86 d 9c 1e 9a	b1 53 :71 :0 00 fd 9 e6 19 5f
Internet Artifact Type Uri Name Uri Host Action Uri Username Element User Password Element Password Value Signon Realm Ssl Valid Preferred	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 00 08 c9c d5 95 f4 37 db e4 00 f1 dc f9 1a 81 9b cb 00 00 02 00 00 20 00 89 ee 7a 7f d6 07 f2 99 8b ce 44 68 50 84 92 51 55 1e 3a 16 6c https://twitter.com 1	n/ sejor_email] @live.com t] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 00 00 00 00 00 00 1 5e ac e8 5a 9c cf 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d 2 96 10 00 00 00 df 34 76 d6 ff 4 e2 1a cc 87 5d 38 59 2d d1 d fe b6 61 d0 13 cb be 42 09 t n/	f c2 97 eb 01 00 00 00 f4 fd df .0 66 00 00 00 01 00 00 20 00 00 3 c 63 1 a 1 c bf fd 73 01 81 85 0 60 4f 72 fa 7 c 91 4 a e7 6f 0e bf 77 bd 07 96 99 2 c 9f 05 cb 7 c fi 25 64 7 d 0 a 8e f5 09 55 4f 4d a 5a 43 79 a2 91 4b a7 9b 4d 0d 9	48 bd 09 8c 4c 0 00 fd 5c 5a 4c 0 00 00 0 e 8 * ff d8 a0 36 37 6 40 00 00 00 4 92 02 e6 86 c 9c 1e 9a	b1 53 :71 0 00 fd 9 e6 J9 Sf
Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value Signon Realm Ssi Valid Preferred Created	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 d0 86 9c d5 95 f4 37 db e4 00 f1 dc f9 1a 81 9b cb 00 00 02 00 00 20 00 89 ec 7a 7f d6 07 f2 09 8b cc 44 68 50 84 92 51 55 1e 3a 16 6c https://twitter.com 1 04/21/13 04:49:59P4	n/ se_or_email] @live.com d df 01.15 d1.11 8c 7a 00 d0 4 0 00 00 00 20 00 00 00 00 00 1 5e ac e8 5a 9c cf 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d 2 96 10 00 00 0df 34 76 cf ff 4 e2 1a cc 87 5d 38 59 2d d1. d fe b6 61 d0 13 cb be 42 09 9 n/	f c2 97 eb 01 00 00 00 f4 fd df 4 0 66 00 00 00 10 00 02 00 00 3c c8 1a 1c bf fd 73 01 81 85 00 60 4f 72 fa 7c 91 4a e7 6f 0e bf 77 bd 07 96 99 2c 9f 05 5c 7c fi 25 64 7d 0a 8e f5 09 55 4f 4d a 5a 43 79 a2 91 4b a7 9b 4d 0d 9	48 bd 09 8c 4c 0 00 fd 5c 5a 4c 0 00 00 00 8 ff d8 a0 36 37 6 40 00 00 00 e 9c 1e 9a	b1 53 ;71 000 fd 9 e6 19 5f
Internet Artifact Type Url Name Url Host Action Url Username Element User Password Element Password Value Signon Realm Ssl Valid Preferred Created Blacklisted	Login Data https://twitter.com twitter.com/ https://twitter.com session[username peterwilson.win8@ session[password 01 00 00 00 00 80 90 d5 95 f4 37 db e4 00 f1 dc f91 a81 9b cb 00 00 02 00 00 20 00 89 ec 7a 7f d6 07 f2 09 8b cc d4 68 50 84 92 51 55 1e 3a 16 66 https://twitter.com 1 1 04/21/13 04:49:59PM 0	n/ sessions e_or_email] @live.com i] d df 01 15 d1 11 8c 7a 00 d0 4 0 00 00 00 02 00 00 00 00 01 5e ac e8 5a 9c d7 72 6f 32 fd 0 00 00 9c ba 49 18 ee d8 7d 1 2 96 10 00 00 df 34 76 d6 ff 4 e2 1a cc 87 5d 38 59 2d d1 d fe b6 61 d0 13 cb be 42 09 s n/	f c2 97 eb 01 00 00 00 f4 fd df4 0 66 00 00 00 00 100 00 20 00 00 3c c8 1a 1c bf fd 73 01 81 85 00 60 4f 72 fa 7c 91 4a e7 6f 0e bf 77 bd 07 96 99 2c 9f 05 cb 7c f 25 64 7d 0a 8e f5 09 55 4f 4d a 5a 43 79 a2 91 4b a7 9b 4d 0d 5	48 bd 09 8c 4c 00 fd 5c 5a 46 000 00 00 0e 8 ff d8 a0 36 37 6 40 00 00 00 e 9c 1e 9a	b1 53 71 0 00 fd 9 e6 19 5f

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:

Live Search Results

⊡ Li	ive Search {"facebook", "twitter"} (ID:1005) performed 07/30/2013 20:11:10 23869 hit(s) in 1898 file(s)
Ē	= Text Query: "facebook" <ansi, case="" insensitive=""> 10820 hit(s) in 1137 file(s)</ansi,>
	🕀 Allocated Space 7713 hit(s) in 802 file(s)
	⊞ Unallocated Space 3107 hit(s) in 335 file(s)
Ē	≟- Text Query: "twitter" <ansi, case="" insensitive=""> 13049 hit(s) in 761 file(s)</ansi,>
	🗄 Allocated Space 9176 hit(s) in 434 file(s)
	⊕ Unallocated Space 3873 hit(s) in 327 file(s)
	Figure 72 Social Media Items
The	e majority of the files that I found that contained mention of either Facebook or Twitter were prima
result of	browsing to websites that contained options to share the contents via Facebook or Twitter. There w

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\ _____

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	
 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 	
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	
Final results of search: Pictures: 42050 items Browser Activity: 2138 items Cloud Services URLs: 3 items Internet Explorer 10 Carved Content Records: 1698 items	
Pictures: 42050 items Browser Activity: 2138 items Cloud Services URLs: 3 items Internet Explorer 10 Carved Content Records: 1698 items	
Browser Activity: 2138 items Cloud Services URLs: 3 items Internet Explorer 10 Carved Content Records: 1698 items	
Cloud Services URLs: 3 items Internet Explorer 10 Carved Content Records: 1698 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 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	@RIT sports	04/21/2013 09:20:53 PM	BB <a data-query-so<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 8.vmdk - Partition 1</th><th>File offset 8882986</th>	Windows 8.vmdk - Partition 1	File offset 8882986
*	2	RIT Sports Info	@RIT sports	04/25/2013 10:47:06 PM	<a data-query-source<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 8. vmdk - Partition 1</th><th>File offset 123181593</th>	Windows 8. vmdk - Partition 1	File offset 123181593
*	3	RIT Sports Info	@RIT sports	04/25/2013 10:45:31 PM	BB <a class="twitter-atreply pretty-link" dandc"="" dir="</th" href="//FisherAthletics"><th>Windows 8.vmdk · Partition 1</th><th>Physical Sector 26768</th>	Windows 8.vmdk · Partition 1	Physical Sector 26768
*	8	RIT Sports Info	@RIT sports	05/04/2013 07:17:30 PM	<a data-query-source<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 8.vmdk · Partition 1</th><th>Physical Sector 26768</th>	Windows 8.vmdk · Partition 1	Physical Sector 26768
★	9	RIT Sports Info	@RIT sports	05/04/2013 07:11:51 PM	<a data-query-source<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 8.vmdk - Partition 1</th><th>Physical Sector 26768</th>	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	@RIT sports	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	@RIT sports	05/04/2013 06:57:06 PM	<a href="//search?q=%23LLWTennisChampionship&src=ha</th><th>Windows 8. vmdk - Partition 1</th><th>Physical Sector 29306</th></tr><tr><th>*</th><th>13</th><th>RIT Sports Info</th><th>@RIT sports</th><th>05/04/2013 06:54:48 PM</th><th><a href=" search?q="%23LLW/TennisChampionship&src=ha</th"><th>Windows 8.vmdk · Partition 1</th><th>Physical Sector 29307</th>	Windows 8.vmdk · Partition 1	Physical Sector 29307
*	16	RIT Sports Info	@RIT sports	05/04/2013 05:52:21 PM	<a class="twitter-atreply</th><th>Windows 8.vmdk - Partition 1</th><th>Physical Sector 29307</th></tr><tr><th>*</th><th>20</th><th>RIT Sports Info</th><th>@RIT sports</th><th>05/04/2013 04:34:42 PM</th><th>BB <a href=" data-query-so<="" href="//search?q=%23LLW/TennisChampionship&src=ha</th><th>Windows 8.vmdk - Partition 1</th><th>Physical Sector 29307</th></tr><tr><th>*</th><th>18</th><th>RIT NEWS</th><th>@RITNEWS</th><th>05/04/2013 05:19:39 PM</th><th>Coverage of <th>Windows 8.vmdk - Partition 1</th><th>Physical Sector 29307</th>	Windows 8.vmdk - Partition 1	Physical Sector 29307
*	23	RIT Sports Info	@RIT sports	05/03/2013 08:56:08 PM	At halftime, <a class="twitter-atreply p</th><th>Windows 8.vmdk - Partition 1</th><th>Physical Sector 43298</th></tr><tr><th>*</th><th>24</th><th>RIT Sports Info</th><th>@RIT sports</th><th>05/04/2013 04:21:47 PM</th><th><a href=" href="/RITMensLax" search?q="%23LLW/TennisChampionship&src=ha</th"><th>Windows 8. vmdk - Partition 1</th><th>Physical Sector 34375</th>	Windows 8. vmdk - Partition 1	Physical Sector 34375
*	25	Windows 7 Forensics	@Win7Forensics	05/01/2013 03:28:57 PM	<a <="" class="twitter-atrepty pretty-link" href="/Win7Forensics" th=""><th>Windows 8. vmdk - Partition 1</th><th>Physical Sector 22051</th>	Windows 8. vmdk - Partition 1	Physical Sector 22051
*	26	RIT Sports Info	@RIT sports	04/21/2013 09:20:53 PM	BB <a data-query-so<="" href="//search?q=%23RIT&src=hash" th=""><th>Windows 8. vmdk - Partition 1</th><th>Physical Sector 97890</th>	Windows 8. vmdk - Partition 1	Physical Sector 97890
*	27	RIT Sports Info	@RIT sports	05/03/2013 08:56:08 PM	At halftime, <a href="/RITMensLax" class="twitter-atreply p</th> <th>Windows 8.vmdk - Partition 1</th> <th>Physical Sector 25220</th>	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 activity. 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).

	All Results	Apr-2013	22	22 24	~	~				May-2013	2	2		
E E	Helmed Heauts Facebook URLs Social Networking Facebook Status Updates. Twitter	20 21 ♦♦ Facebook URLs	22	23 24	25	25	27 2	8 29	30			3	4 :	6
				ļ								I		
		Facebook Status	s updates/wa	Il Posts/Comments										
													1	
		◆◆ Twitter												
										V				
		1-Apr-2013	11-Ap	-2013	21-Apr-2013		1-May-201		11-May-2013		21-May-2	013	31-M	ay-2013
		All Results			+	↓	++							
							1							



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:



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 <u>peterwilson.win8@gmail.com</u>, 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:

xpiore Overview Email Graphics Bookmarks Live Sean	ch Ind	ex Search Volable	e						_
Email Items	File List		_			Diselau Tina Zan	- Factors Daulists Time (Face lead an shire)		
Email Status	합하	07 🖊 🖬 🛽			🗐 📺 🛄 Email	 Display Time Zone 	e: Eastern Daylight Time (Pronhocal machine)		- 4)
Email Archives		 Name 		Submit Time	Subject		То		
Email by Date		20000066_3b87	e4aab32b0.eml	4/21/2013 3:	04/21/2013 Daily Email		Windows7 Gmail <peterwilson.win7@gmail.com>, V</peterwilson.win7@gmail.com>	Vindows8 Gmail <peterwilson.win< td=""><td>18@gma</td></peterwilson.win<>	18@gma
Email Addresses		20000067_5529	4a730e486.eml	4/21/2013 4:	Microsoft account security in	fo confirmation	<pre><peterwilson.win8@gmail.com></peterwilson.win8@gmail.com></pre>		
- Senders [From] (87 / 87)		20000068_aed0	3a1b3c856.eml	3/7/2013 12:	Get Gmail on your mobile pho	ne	Peter Wilson <peterwilson.win8@gmail.com></peterwilson.win8@gmail.com>		
- 🔚 Recipients [To, CC, BCC] (87 / 87)		20000069_5184	0818891af4.eml	3/7/2013 12:	Import your contacts and old	email	Peter Wilson <peterwilson.win8@gmail.com></peterwilson.win8@gmail.com>		
To" Recipients (87 / 87)		2000006a_4e63	ca7a21641.eml	3/7/2013 12:	Customize Gmail with colors a	ind themes	Peter Wilson <peterwilson.win8@gmail.com></peterwilson.win8@gmail.com>		
E- Email Domains [2/2]		2000006b d347	8487c92a3f.eml	3/7/2013 12:	Getting started on Google+		<pre><peterwilson.win8@gmail.com></peterwilson.win8@gmail.com></pre>		
⊞		2000006c d9319	99e745aa8d.eml	3/7/2013 12:	Welcome to Facebook - get s	tarted now!	WindowsEight Forensics <peterwilson.win8@gmail.c< td=""><td>om≥</td><td></td></peterwilson.win8@gmail.c<>	om≥	
E Call Email Addresses (87 / 87)		2000006d d353	d7a4f7de7.eml	3/7/2013 12:	Just one more step to get st	arted on Facebook	<pre><peterwilson.win8@gmail.com></peterwilson.win8@gmail.com></pre>		
 peterwilson.win7@gmail.com (28 / 28) 		2000006e 117b	b96f645ad3.eml	3/7/2013 12:	peterwilson.win8@live.com	added to your Facebook accoun	t WindowsEight Forensics <peterwilson.win8@gmail.c< td=""><td>>m></td><td></td></peterwilson.win8@gmail.c<>	>m>	
peterwiison.win7@live.com (26 / 26)		2000006f 58d98	3b439adc57.eml	3/7/2013 12:	WindowsSeven Forensics wa	nts to be friends on Facebook	WindowsEight Forensics <peterwilson.win8@amail.c< td=""><td>om></td><td></td></peterwilson.win8@amail.c<>	om>	
peterwison.wind@gmail.com(46/46)		20000070 857d	7b4e71bb66.eml	3/7/2013 1:1	Peter Wilson confirmed you a	is a friend on Eacebook	WindowsEight Earensics < peterwikson.win8@amail.c	< mc	
In the second		20000071 bdde	69hc4afd22.eml	3/7/2013 1:1	niw5578@mailtest.rit.edu.ac	ded to your Eacebook account	WindowsEight Forensics < neterwikon.win8@amail.c	nn>	
The contract of the contract o		20000072 7665	727d5ad786.eml	3/7/2013 1-2	Tech		cheterwijson win8@gmail.com>		
BCC Reaplents (0/0)		20000073 6891	f87ca23bf8.eml	3/25/2013 6:	Top 3 posts for you on Goog	e+ this week	<pre>cpeterwisen win8@gmail.com></pre>		
Email Domains [2 / 2]		20000075_0071	rdsf5590hc emi	3/7/2013 1-2	Tert	OT UID WOOK	<pre>cpeterwilcon win8@gmail.com></pre>		
Email Advances (97/97)		20000078_c120	coor or you crowl	4/21/2012 2:	04/21/2012 Daily Email		Windows7 Cmail «DetertWiscon Win7@amail.com>	Undows? Croal «DebarkWison Wire	-0/0
Email (87/87)	H	20000076_care	1756b22014 ord	4/21/2013 3	04/21/2013 Daily Lindi		Windows/ Ginal <peter @ginal.com="" win="" wison=""></peter> , <	VindowsSource Encoder vision. With	Alcon 1
Endar(or y or y		2000007_0490	0e1deE9677.eml	4/21/2012 4:	04/21/2013 Daily Entail		Windowso Ginal «Peter Wison Windogginal.com», 4	VindowsSeven Forensics <peter td="" w<=""><td>Alson '</td></peter>	Alson '
		20000000_0774	ocación de la companya de la compa	4/22/2013 1	Tap 3 parts for you on Coop	le t this meals	vantowso dinar receivisor. winograi.com/, </</td <td>vindowsbeven r orensics <td>15015</td></td>	vindowsbeven r orensics <td>15015</td>	15015
		20000000_2105	seeu21155.em	4/22/2013 0:	nup 5 posts for you of Goog	et uis week	<pre><pre>cprcerwison.winoggital.com></pre></pre>	dense og de se transfere autom	
		20000130_#330	dr4699d.em	4/23/2013 10	04/23/2013 Daily Email		windows/ Live <peterwison.win @ive.com="">, win</peterwison.win>	dowse Gmail <peterwilson, td="" windle<=""><td>/gmail</td></peterwilson,>	/gmail
		20000133_rba02	20090ad063.emi	4/24/2013 9:	04/24/2013 Email with Attack	imenc	windows/ Gmail <peterwison. @gmail.com="" win="">, *</peterwison.>	windowso Gmail < Peter wilson. win	10@gn
		20000134_9400	48UabC9DC9.emi	4/23/2013 10	04/23/2013 Daily Email		windows/ Live <peterwison.win @ive.com="">, win</peterwison.win>	dowsb Gmail <peterwilson, td="" windlig<=""><td>-gmail</td></peterwilson,>	-gmail
		20000135_c3cf2	298d6385c.eml	4/24/2013 9:	04/24/2013 Email with Attack	hment	Windows7 Gmail <peterwilson.win7@gmail.com>, 1</peterwilson.win7@gmail.com>	Vindows8 Gmail <peterwilson.win< td=""><td>18@gn</td></peterwilson.win<>	18@gn
		20000137_a701	0e76a406b2.eml	4/24/2013 9:	04/24/2013 Email with Attack	nment	WindowsSeven Forensics <peterwilson.win7@live.c< td=""><td>om>, WindowsSeven Forensics <</td><td>Peter</td></peterwilson.win7@live.c<>	om>, WindowsSeven Forensics <	Peter
		20000138_698e	2ec6d1774F.eml	4/24/2013 9:	04/24/2013 Email with Attack	nment	WindowsSeven Forensics <peterwilson.win7@live.c< td=""><td>om>, WindowsSeven Forensics <</td><td>Peter</td></peterwilson.win7@live.c<>	om>, WindowsSeven Forensics <	Peter
		2000013b_14da	Sfec214f8d.eml	4/25/2013 9:	04/25/2013 Daily Email		Windows8 Gmail <peterwilson.win8@gmail.com>, \</peterwilson.win8@gmail.com>	Vindows8 Live <peterwilson.win8< td=""><td>;@live.</td></peterwilson.win8<>	;@live.
		2000013c_2696	6230867c72.eml	4/25/2013 9:	04/25/2013 Daily Email		Windows8 Gmail <peterwilson.win8@gmail.com>, V</peterwilson.win8@gmail.com>	Vindows8 Live <peterwilson.win8< td=""><td>@ive</td></peterwilson.win8<>	@ive
		20000145_31cf9	9de9378a84.eml	4/26/2013 11	04/26/2013 Daily Email		Windows7 Gmail <peterwilson.win7@gmail.com>, \</peterwilson.win7@gmail.com>	Vindows8 Gmail <peterwilson.win< td=""><td>18@grr</td></peterwilson.win<>	18@grr
		20000146_dc9d	57e672d4cc.eml	4/26/2013 11	04/26/2013 Daily Email		Windows7 Gmail <peterwilson.win7@gmail.com>, \</peterwilson.win7@gmail.com>	Vindows8 Gmail <peterwilson.win< td=""><td>18@gm</td></peterwilson.win<>	18@gm
		20000148_fb3a4	4a17d5292.eml	4/26/2013 11	04/26/2013 Daily Email		Windows8 Gmail <peterwilson.win8@gmail.com>, F</peterwilson.win8@gmail.com>	eter Wilson <peterwilson.win8@l< td=""><td>dive.co</td></peterwilson.win8@l<>	dive.co
		20000149_8b41	4805342d3c.eml	4/26/2013 11	04/26/2013 Daily Email		Windows8 Gmail <peterwilson.win8@gmail.com>, F</peterwilson.win8@gmail.com>	eter Wilson <peterwilson.win8@l< td=""><td>live.co</td></peterwilson.win8@l<>	live.co
		2000014a_451e	528741b578.eml	4/26/2013 11	04/26/2013 Daily Email		Windows8 Gmail <peterwilson.win8@gmail.com>, F</peterwilson.win8@gmail.com>	eter Wilson <peterwilson.win8@l< td=""><td>dive.co</td></peterwilson.win8@l<>	dive.co
	1	20000152 2020	at date 2 ad and	x100/0010.0.	04/00/0010 Doll - Emol		Windows71iva_zDatorWilson_Win7@liva_com>Win	dawel Consil Makadilikaan Winla	ite erect
	Loadeo	1: 46 Fi	Itered: 46	Total: 46	Highlighted: 0	Checked: 0 Total	LSize: 152.5 KB		

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

In the case of email sent to <u>peterwilson.win8@live.com</u>, 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:

Creed Bases	-				
Email Items	File List			Dislay Ting Tang	Festers Daulisht Time (Peru least anabias)
🕀 🔜 Email Status	- da 9	ê 🖊 🔒 🔳	• •	Email Usplay Time Zone:	Eastern Daylight Time (From local machine) 👘 者 🗶 🔅
🗄 🖅 Email Archives		 Name 	Submit Time	Subject	To
🗈 🔚 Email by Date		20000066_3b87e4aab32b0.eml	4/21/2013 3:	04/21/2013 Daily Email	Windows7 Gmail <peterwilson.win7@gmail.com>, Windows8 Gmail <peterwilson.win8@gmail.co< td=""></peterwilson.win8@gmail.co<></peterwilson.win7@gmail.com>
🖃 🖼 Email Addresses		20000074_c65a2b3243aebc.eml	3/7/2013 1:4	Confirm your Twitter account, Win8Forensics!	Windows 8 Forensics <peterwilson.win8@live.com></peterwilson.win8@live.com>
😟 🖾 Senders [From] (87 / 87)		20000076 4040e689bf019c.eml	3/7/2013 12:	Facebook Email Verification	WindowsEight Forensics <pre>cpeterwilson.win8@live.com></pre>
🖻 🖼 Recipients [To, CC, BCC] (87 / 87)		20000077_3bb4833a7cb5bf.eml	3/7/2013 12:	Getting started with Hotmail	cneterwikon win8@live.com>
To" Recipients (87 / 87)		20000078_cp1cco4727225_cml	4/21/2012 21	04/21/2012 Dalu Email	Windows? Crasil «DeterWilcon Win?@gmail.com», Windows? Crasil «DeterWilcon Win?@gmail.co
Email Domains [2 / 2]		20000078_CaleCe4727225.em	4/21/2013 3:	04/21/2015 Daily Elitai	windowsz ginal częcerwison, winzgginal.comz, windowsz ginal częcerwison, winogginal.co
F - C Display Name (87 / 87)		20000079_See29b7aeb2aed.emi	4)21)2013 4:	You ve connected Google to your Microsoft account	<peterwilson.winbiguive.com></peterwilson.winbiguive.com>
E-THE Email Addresses (87 (87)		2000007a_81831968F9d1F9.eml	4/21/2013 4:	Confirm your Twitter account, Win8Forensics!	Windows 8 Forensics <peterwilson.win8@live.com></peterwilson.win8@live.com>
peterwikan win7@amail.com (28 / 28)		2000007b_7a2be7be367c95.eml	4/21/2013 4:	You've connected Facebook to the People app	<peterwilson.win8@live.com></peterwilson.win8@live.com>
pecervision.win/@gmail.com (20/20) pecervision.win7@bus sees (26/26)		2000007c_878908ce90d155.eml	4/21/2013 4:	You've connected Twitter to the People app	<peterwilson.win8@live.com></peterwilson.win8@live.com>
pecervitisen win/@river.com (26/26) pecervitisen win/@river.com (26/26)		2000007e_14569a6a2fd0ca.eml	4/21/2013 4:	Please sign in to your account	<pre><peterwilson.win8@live.com></peterwilson.win8@live.com></pre>
Call peterwister. wir olgginal.com (46 / 46)		20000081_22dae5eecdeaf3.eml	4/21/2013 4:	Get to know your new inbox	<pre>cpeterwison.win8@live.com></pre>
pererwisch.windgilve.com (63,63)		200000rd_a883635714023a.eml	4/23/2013 10	04/23/2013 Daily Email	Peter Wilson <neterwilson win8@live.com="">. WindowsSeven Earensics <peterwilson td="" win7@amail<=""></peterwilson></neterwilson>
CC Recipients (2) 2)		200000co_1o7910cco226Ef.cml	4/22/2012 10	04/22/2012 Daily Email	Dater Witcon contenuitors win9@ine com>, WindowsFarers Exercises cillaterWitcon Win7@email
BCC Recipients (U/U)		200000te_te/otoeca30001.em	4/20/2010 10	04/23/2013 Daily Email	Peter wison specerwison winogave.com/, windowspevern dierbics specerwison winoganal
Email Domains [2 / 2]		20000130_1133cu 46990.em	4/25/2015 10	04/25/2015 Daily Enail	windows/ twe creter wison, win/give.com/, windows/ Ginal creter wison, winogginal.com/
Display Name (87 / 87)		20000131_6c542a47819a68.eml	4/24/2013 1:	Windows 8 Forensics, complete your 1 witter profile today!	Windows 8 Forensics <peterwison.win8@live.com></peterwison.win8@live.com>
Call Email Addresses (87 / 87)		20000132_4c6799a7b8b17.eml	4/24/2013 1:	Get Twitter on your mobile phone	Windows 8 Forensics <peterwilson.win8@live.com></peterwilson.win8@live.com>
		20000133_fba026d95ad063.eml	4/24/2013 9:	04/24/2013 Email with Attachment	Windows7 Gmail <peterwilson.win7@gmail.com>, Windows8 Gmail <peterwilson.win8@gmail.co< td=""></peterwilson.win8@gmail.co<></peterwilson.win7@gmail.com>
		20000134_94bb480a6c9bc9.eml	4/23/2013 10	04/23/2013 Daily Email	Windows7 Live <peterwilson.win7@live.com>, Windows8 Gmail <peterwilson.win8@gmail.com></peterwilson.win8@gmail.com></peterwilson.win7@live.com>
		20000135_c3cf2298d6385c.eml	4/24/2013 9:	04/24/2013 Email with Attachment	Windows7 Gmail <peterwilson.win7@gmail.com>, Windows8 Gmail <peterwilson.win8@gmail.co< td=""></peterwilson.win8@gmail.co<></peterwilson.win7@gmail.com>
		20000139_d60adfe7d5e49.eml	4/25/2013 3:	Windows 8 Forensics, find your friends on Twitter!	<pre><peterwilson.win8@live.com></peterwilson.win8@live.com></pre>
1		2000013a d59fcaa4b5f549.eml	4/25/2013 6	Get started with Windows	<pre>cpeterwilson.win8@live.com></pre>
1		2000013h 14da5far214f8d and	4/25/2013 9	04/25/2013 Daily Email	Windows8 Gmail «PeterWilson Win8@gmail.com» Windows8 Live «DeterWilson Win9@live com»
1		20000130_11003080219100.8MI	4/05/2010 9:	04/25/2012 Daily Lindi	Windows and SteterWisen Windows (cm2) Windows Live SteterWiser, Windows (cm2)
1		20000130_2096623086/C/2.em	4/25/2013 9:	organization party Email	windows6 unial <peterwison.win8@live.com>, Windows6 Live <peterwison.win8@live.com></peterwison.win8@live.com></peterwison.win8@live.com>
1		200013e_b7e504ca78bc6b.eml	4/25/2013 10	04/25/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com>, Windows5even Forensics <peterwilson.win7@gmail< td=""></peterwilson.win7@gmail<></peterwilson.win8@live.com>
1		2000013f_6eb38099c703bc.eml	4/25/2013 10	04/25/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com>, Windows5even Forensics <peterwilson.win7@gmail< td=""></peterwilson.win7@gmail<></peterwilson.win8@live.com>
		20000143_42dbe1aec0b20.eml	4/25/2013 10	Fw: 04/25/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com>
1		20000144_d889e948eb621a.eml	4/25/2013 10	Fw: 04/25/2013 Daily Email	Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com>
		20000145 31cf9de9378a84 emi	4/26/2013 11	04/26/2013 Daily Email	Windows7 Gmail <peterwilson.win7@gmail.com>. Windows8 Gmail <peterwilson.win8@gmail.co< td=""></peterwilson.win8@gmail.co<></peterwilson.win7@gmail.com>
		20000146 dc9d57e672d4cc eml	4/26/2013 11	04/26/2013 Daily Email	Windows7 Gmail <peterwilson.win7@gmail.com>. Windows8 Gmail <peterwilson.win8@gmail.com< td=""></peterwilson.win8@gmail.com<></peterwilson.win7@gmail.com>
		20000148 Fb3s4s174E302!	4/26/2012 11	04/26/2013 Daily Email	Vindows8 Gnail / PeterWilcon Win8@gnancom>, Deter Wilcon / DeterWilcon Win8@glidi.LU
		20000110_0001d1/00292.6M	420/2010 11	04/06/2010 Daily Lindi	Water with the second s
		20000149_80414805342d3c.em	*/26/2013 11	unizoiz013 Daily Email	windowso unial <peterwilson.windgrgmail.com>, Peter Wilson <peterwilson.win8@live.com>,</peterwilson.win8@live.com></peterwilson.windgrgmail.com>
		200014a_451e528741b578.eml	4/26/2013 11	04/26/2013 Daily Email	Windowsti Gmail <peterwilson.win8@gmail.com>, Peter Wilson <peterwilson.win8@live.com>,</peterwilson.win8@live.com></peterwilson.win8@gmail.com>
		2000014+ 1ED/E716-MEDFd and	4/26/2012 12	Dec 04/26/2012 Date Enail	Dates Wilson Anatomileon win0@live comb
		Figure ov Ei	nan se	in to peter witson.wind	
Explore Overview Email Graphics Bookmarks Live Se	earch Ind	ex Search Volatile			
					4
EmailItems	File List	a / .	v 📰 v	Display Time Zone	ہ : Eastern Daylight Time (From local machine) 🛛 🙀 🔧 😪
Email Status	File List		v ≣•	Display Time Zone	: Eastern Daylight Time (From local machine) 👘 🎢 💥 🗇
Email Rems 4	File List	2 / 1	▼ 📰 ▼	Display Time Zone	: Eastern Daylight Time (From local inschine)
Email Items 9 Email Status Email Archives Email Archives Email and by Date	File List	Image: Constraint of the second sec	Submit Time 4/25/2013 10	Emai Emai Display Time Zone Subject Fw: 04/25/2013 Daily Email	4 : Eastern Daylight Time (From local machine) 👘 🏄 💥 🗇 🔺 To Peter Wilson <peterwilson.win@gilve.com></peterwilson.win@gilve.com>
Email Items 4 Email Items 4 Email Renail Status Email Archives Email Addresses Email Addresses Email Addresses		Image: Constraint of the second sec	Submit Time 4/25/2013 10 4/26/2013 12	Email Display Time Zone Subject - FW: 04/25/2013 Daily Email - Re: 04/26/2013 Daily Email -	Eastern Daylight Time (From local machine)
Email Items 4 Imail Status Imail Status Imail Archives Imail Archives Imail Email by Date Imail Archives Imail Email by Date Imail Archives Imail Email by Date Imail Email Archives Imail Email Archives Imail Email Archives Imail Email Brown (KF / S7) Imail Email Archives		Name 20000144_d889e948eb621a.em 2000014c_159d571bdd58fd.em 20000150_fd443a615a8c1f.em	 Submit Time 4/25/2013 10 4/26/2013 12 4/26/2013 12 	Comparison C	4 Eastern Daylight Time (From local machine) To To Peter Wilson <peterwilson, win8@lvvs.com=""> Peter Wilson <peterwilson <pre="">win8@lvvs.com> Peter Wilson <peterwilson <pre="">win8@lvvs.com> </peterwilson></peterwilson></peterwilson,>
Enail Items 1 Imail Items 1		Name 20000144_d889e949eb621a.eml 20000150_f4443ae153e8c1f.eml 20000150_f4443ae153e8c1f.eml 20000162_27f2fc5d5c9a-7.eml	▼ ■ ▼ Submit Time 4/25/2013 10 4/26/2013 12 4/26/2013 12 5/1/2013 11	Subject Display Time Zone Subject Wey Of 25(2013 Daily Email Re: 04(26(2013 Daily Email Fw: 04(26(2013 Daily Email))))))))))))))))))))))))))))))))))))	Eastern Daylght Time (From local machine) Eastern Daylght Time (From local machine) To Peter Wison opeterwison.win@Bl/ve.com> Peter Wison opeterwison.win@Bl/ve.com> Peter Wison opeterwison.win@Bl/ve.com> Exter Wison opeter Wison opeter Wison opeter Wison opeter Wison opeterwison.win@Bl/ve.com> Exter Wison opeter Wison opeter
Enail Zens 1 0:		Name 20000144_d839e9498eb621a.em/ 20000150_fd43aef53ecf.em/ 20000150_fd43aef53aecf.em/ 20000152_272fc5d5c9a7.em/ 20000155_dd6ec228225a5b.em/	▼ ■ ▼ Submit Time 4/25/2013 10 4/26/2013 12 4/26/2013 12 5/1/2013 11 5/1/2013 11	Display Time Zone Sobject Fw: 04/25/2013 Daly Enal Re: 04/26/2013 Daly Enal Re: 04/26/2013 Daly Enal Re: 04/26/2013 Daly Enal Re: 05/10/2013 Daly Enal Hour Solution	Eastern Daylight Time (From local machine) To Peter Wilson cpeterwilson.win8@live.com> Peter Wilson cpeterwilson.win8@live.com> Peter Wilson cpeterwilson.win8@live.com> s s Peter Wilson cpeterwilson.win8@live.com> s s s Peter Wilson cpeterwilson.win8@live.com> s s s s s s s s s s s s s s s s s s s
Enail Remis 1 If and Remis 1 If and Achroses If and Achroses If and Achroses If and Achroses If and Achroses If and Achroses (11 / 11) If and Achroses (7 / 87) If and Achroses (7 / 87)		Name 2000014_d839e348ab621a.eml 2000014_d1596471bd58f6.dml 20000150_fd443ae15a8c1f.eml 20000162_2776fc545v9ea7.eml 20000165_2056c28235a5b.eml 20000196_d8bds67817.eml	Submit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11: 5/1/2013 11: 5/1/2013 11: 5/3/2013 7:2	Subject Subject Subject Subject Subject Subject Subject Sec 04(25(2013 Daly Email Five: 04(25(2013 Daly Email Five: 04(25(2013 Daly Email Five: 04(25(2013 Daly Email Five: 05(10)(2013 Daly E	Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) Peter Wison opeterwison.win8@kve.com> Peter Wison opeterwison.win8@kve.com> Peter Wison opeterwison.win8@kve.com> Se Peter Wison opeterwison.win8@kve.com> Se Peter Wison opeterwison.win8@kve.com>
Enal Rens 1 C Enal Actives Enal Actives Enal Actives Enal Actives Enal Actives Enal Actives Enal Actives Enal Actives		Name 20000144_d839e9498eb621a.eml 20000150_f4443e15ae51f.eml 20000150_f4443e15ae51f.eml 20000162_d2762f6549e87.eml 20000162_d266e2823545b.eml 20000169_d5b6e838e67617.eml	✓ ■ ✓	Dupley Time Zone Subject Fiv: 04/25/2013 Daly Email Re: 04/26/2013 Daly Email Re: 04/26/2013 Daly Email Re: 05/26/2013 Daly Email	2 Eastern Daylght Time ('from local machine) Category Constraints ('from local machine) Category Constraints ('from local machine) Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.win8@live.com> Sea Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterw
Tenal Rems 1 Imal Rems 1 Imal Probes 1 Imal Probs		Name 20000144_d889e948eb621a.em/ 20000144_d889e948eb621a.em/ 20000156_d44as15se61.em/ 20000165_d24as15se61.em/ 20000165_d26e38567617.em/ 2000019f_e2b44bec38567617.em/ 2000019f_e2b44bec38567617.em/	♥ ■ Submit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 71 5/3/2013 72 5/3/2013 72 4/26/2013 12	Subject Final Display Time Zone Subject Finu 04/25/2013 Daily Email Finu 04/25/2013 Daily Email Finu 04/25/2013 Daily Email Finu 04/25/2013 Daily Email Finu 05/2012 Daily Email whit Text and Picture Attachment Finu 05/2012 Daily Email Finu 05/2012 Daily Email Finu 05/2012 Daily Email	Eastern Daylght Time (From local machine) Eastern Daylght Time (From local machine) Peter Wison cpeterwison.win8@kve.com> Peter Wison cpeterwis
Enail Zens 1 Image: Status Image: Status Image: Status		Name 20000144_d839e9498e5621a.em 20000150_f1443as15abc11.em 20000150_f1443as15abc11.em 20000150_f1443as15abc11.em 20000150_g443as15abc11.em 20000150_g465c223535b.em 2000019f_g45b4bc3364.em 2000019f_g45b4bc3364.em 20000143_a12abc1aectbac2.em	♥ ■ ▼ ■ ■ ■ ▼ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	Dupley Time Zone Sobject Fiv: 04/25/2013 Daly Enal Re: 04/26/2013 Daly Enal Re: 04/26/2013 Daly Enal Re: 05/26/2013 Daly Enal Re: 05/26/2013 Daly Enal Re: 05/2013 Daly Enal Re: 05/2013 Daly Enal Re: 05/2013 Daly Enal Fiv: 04/26/2013 Daly Enal Fiv: 04/26/2013 Daly Enal Fiv: 04/26/2013 Daly Enal Fiv: 04/26/2013 Daly Enal	Eastern Daylght Time ('from local machine) Eastern Daylght Time ('from local machine) To Peter Wilson cpeterwilson.win8@lyke.com> Peter Wilson cpeterwilson.win8@lyke.com> Peter Wilson cpeterwilson.win8@lyke.com> Se Peter Wilson cpeterwilson.win8@lyke.com> Peter Wilson cpeterwils
Enal Rens 1 E Enal Status E Enal Actives		Name 20000144_d889e748eb621a.em 20000146_159677bd587d.em 20000165_d7443e15be81f.em 20000162_d773fc565c9ea7.em 20000162_d745c565c9ea7.em 2000019f_e2bd4bec38fc7817.em 2000019f_e2bd4bec38fc7817.em 20000141_g77d5766305s6d.em	▼ Image: The second seco	Subject Final Display Time Zone Subject Final Display Enal Re: 04(25)(2013 Daily Enal Re: 05(2013 Daily Enal Re: 05(01)(2013 Daily Enal With Text and Picture Attachmen Finu: 05(01)(2013 Daily Enal With Text and Picture Attachmen Finu: 05(03)(2013 Daily Enal Finu: 04(25)(2013 Daily Enal Re: 04(26)(2013 Daily Enal	2 Eastern Daylght Time (From local machine) Eastern Daylght Time (From local machine) Not the second
Enal Rens 1 ● ■	50 Fle List.	Name 20000144 4,38949498cb61a 4,38949498cb61a 2000145 2,986271bd588fd emil 2000159 2,94625571bd588fd emil 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562714 2000159 2,94624562744667 2000159 2,94624562744667 2000159 2,9462555646 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244667 2000159 2,946255244676 2000159 2,94625524567 2000159 2,94625524567 2000159 2,9462555556 2000159 2,9462555556 2000159 2	V Estimation \$ubmit Time 4/25/2013 10 4/26/2013 12 4/26/2013 12 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/3/2013 72 4/25/2013 12 4/25/2013 12 4/25/2013 12 4/25/2013 12	Dupley Time Zone Subject Fiv: 04/25/2013 Daily Enail Re: 04/26/2013 Daily Enail Re: 04/26/2013 Daily Enail Re: 05/26/2013 Daily Enail Re: 05/26/2013 Daily Enail Re: 05/26/2013 Daily Enail Fiv: 06/26/2013 Daily Enail Fiv: 04/25/2013 Daily Enail Fiv: 04/25/2013 Daily Enail Re: 04/26/2013 Daily Enail Fiv: 04/26/2013 Daily Enail	Eastern Daylight Time ('from local machine) Eastern Daylight Time ('from local machine) To Peter Wilson cpeterwilson.win8@live.com> Peter Wilson cpeterwils
Enail Rens 1 Imail Status 1 Imail Northwes 1 Imail Do Date 1 Imail Do Date 1 Imail Do Date 1 Imail Do Date 1 Imail Contrast (11 / 11) 1 Imail Do Date 1 Imail Dotte 1		Name Name 2000014 JS896498b521a.em 200014 JS8971bd588fd.em 200018 JS8671bd58fd.em 200018 ZM5655e31.em 200019 JS867867511 200019 JS8649867511 200019 JS8649867511 200019 JS8649867511 2000114 JS76508564 2000114 JS65498673894 2000114 JS654946673946	▼ ₩ ▼ Submit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 7:2 5/3/2013 7:2 4/25/2013 10 4/25/2013 10 4/25/2013 12 5/1/2013 11	Coppley Time Zone Subject Five 04/25/2013 Daily Email Five 04/25/2013 Daily Email Re: 04/25/2013 Daily Email Re: 05/01/2013 Daily Email with Text and Picture Attachment Five: 05/01/2013 Daily Email with Text and Picture Attachment Five: 05/03/2013 Daily Email with Re: 04/26/2013 Daily Email Re: 04/26/2013 Daily Email Re: 04/26/2013 Daily Email Re: 04/26/2013 Daily Email	2 Eastern Daylght Time (from local machine) Eastern Daylght Time (from local machine) To Peter Wilson opeterwison.win8@kva.com> Peter Wilson opeterwison.win8@kva.com>
Enail Zens		Name 2000144 4,38949486521a.em 2000144 4,38949486521a.em 2000152 2000150 1/4434513621f.em 2000152 2000152 2/425452835.eff.em 2000152 2000154 2/425425355b.em 2000156 2000154 2/425425355b.em 2000156 2000154 2/425425355b.em 2000156 2000154 2/525555667.em 2000164 20000164 4/55652672.em 2000164	Submit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 12 5/3/2013 7:2 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11	Display Time Zone Solvert Pro: 04/25/2013 Daily Enal Re: 04/26/2013 Daily Enal	2 Eastern Daylight Time ("from local machine) Eastern Daylight Time ("from local machine) Not the set of the
Enail Rens Total Rens T		Name 2000014 JS8964980b521a.em 2000014 JS8971bd6387d.em 200018 JS645568cf.em 200018 JS645568cf.em 200018 JS645568cf.em 200019 JS6456568cf.em 200019 JS6456568cf.em 200019 JS6456568cf.em 200019 JS6456568cf.em 200019 JS645668cf.em 2000114 JS756630586d.em 2000114 JS756630586d.em 2000114 JS765630586d.em 2000114 JS7656305864	▼ ₩ Submit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/1/2013 11 5/3/2013 7:2 5/3/2013 7:2 4/25/2013 10 5/3/2013 7:2 5/3/2013 7:2 4/26/2013 12 5/1/2013 11 5/1/2013 11 5/1/2013 12 5/1/2013 12 5/1/2013 12 5/1/2013 12 5/3/2013 7:2	Coppley Time Zone Subject For: 04/25/2013 Daily Email For: 04/25/2013 Daily Email Re: 04/25/2013 Daily Email Re: 05/01/2013 Daily Email Re: 05/01/2013 Daily Email For: 05/01/2013 Daily Email For: 04/25/2013 Daily Email For: 04/25/2014 For: 04/25	2 Eastern Daylght Time (From local machine) E Eastern Daylght Time (From local machine) ▲ To Peter Wilson opeterwilson.win8@kve.com> Peter Wilson
Enail Rens Imail Rens		Name 200014 19874 200014 19874 200014 19874 200014 19874 200014 19874 2000150 144326 2000165 2062225555 2000166 2062225555 2000167 20545564721 2000143 1956935564 2000144 276755564 2000144 19569556472 20000144 19569356856712 20000154 195693263202 20000154 195693263202 20000154 195693263202 20000154 195693263202 20000154 195693263202		Display Time Zone Solvert First 04/25/2013 Daily Enal Ret 04/26/2013 Daily Enal	2 Eastern Daylight Time ("from local machine) Eastern Daylight Time ("from local machine) No. 10 Peter Wilson cpeterwilson.win8@kve.com> Peter Wilson cpeterwilson.win8@kve.com>
Enail Rens 1 Imail Status 1 Imail Archees 1 Imail Do Dee 1 Imail Do Dee 1 Imail Archees 1 Imail Do Dee 1 Imail Do Dee 1 Imail Archees 1 Imail Do Dee 1 Imail Domars [11 / 11] 1 Imail Domars [17 / 17] 1 <t< td=""><td></td><td>Name 2000014 JS8964980b521a.em 2000014 JS8971bd5887d.em 200018 JS8671bd5887d.em 200018 Z9674556827.em 200018 Z9674556827.em 200019 Z9649687417.em 200019 Z9649687417.em 2000114 JS76766325864 2000114 JS7676632544667 2000114 JS7676632544687 2000114 JS7676632749687 2000114 JS7676632749687 20000114 JS767663274967 20000114 JS767663274967 20000114 JS767663274967 20000114 JS767663274967 20000114 JS767663274967 20000114 JS7677663274967 20000114 JS767749274967</td><td></td><td>Display Time Zone Subject Find Find</td><td>2 Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win8@live.com> Peter Vilson opeterwilso</td></t<>		Name 2000014 JS8964980b521a.em 2000014 JS8971bd5887d.em 200018 JS8671bd5887d.em 200018 Z9674556827.em 200018 Z9674556827.em 200019 Z9649687417.em 200019 Z9649687417.em 2000114 JS76766325864 2000114 JS7676632544667 2000114 JS7676632544687 2000114 JS7676632749687 2000114 JS7676632749687 20000114 JS767663274967 20000114 JS767663274967 20000114 JS767663274967 20000114 JS767663274967 20000114 JS767663274967 20000114 JS7677663274967 20000114 JS767749274967		Display Time Zone Subject Find	2 Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win8@live.com> Peter Vilson opeterwilso
Enail Rens In India Rens India Ind		Name 200014 19874 200014 19874 200014 19874 200014 19874 200014 19874 200014 19874 200014 19874 2000150 144345 2000162 2062225555 2000194 2767565564 2000194 2767565564 2000194 2767565564 2000194 2767565564 2000194 27675432830. 20000194 2767343330. 20000194 2767343330. 20000194 2767343330. 20000194 2767343330.		Display Time Zone Solvert First 04/25/2013 Daily Enal Ret 04/26/2013 Daily Enal	2 Eastern Daylight Time ("from local machine) E Eastern Daylight Time ("from local machine) Peter Wilson opeterwilson.win8@kve.com> Peter Wilson opeterwilson.win
Enail Rens 1 Imail Status 1 Imail Advises 1 Imail Do Dee 1 Imail Advises 1 Imail Do Dee 1 Imail Domers [11 / 11] 1 Imail Domers [17 / 17] 1 <td< td=""><td></td><td>Name 2000014 (38969486b521a.em) 2000014 (389671bd5867d.em) 200018 (376455e817.em) 200018 (376455e817.em) 200018 (376455e817.em) 200018 (376455e817.em) 200018 (3764565837.em) 200018 (3764565837.em) 200018 (3764565837.em) 200018 (3764565837.em) 200018 (37645658.em) 200019 (37645658.em) 200019 (37645658.em) 200019 (376456387.em) 200019 (37647668387.em) 200019 (376476683714.em) 200019 (376476683714.em) 200019 (376476683714.em) 200019 (3764766832.em)</td><td>♥ (■♥) Sudmit Time 4/25/2013 10. 4/26/2013 12. 5/1/2013 11 5/1/2013 11 5/3/2013 72 4/25/2013 12 4/25/2013 12 5/3/2013 72 5/3/2013 72 4/25/2013 12 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 5/3/2013 72 5/</td><td>Display Time Zone Subject Find Find Copplay Time Zone Subject Find Fi</td><td>2 Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win8@live.com> Peter Vilson opeterwils</td></td<>		Name 2000014 (38969486b521a.em) 2000014 (389671bd5867d.em) 200018 (376455e817.em) 200018 (376455e817.em) 200018 (376455e817.em) 200018 (376455e817.em) 200018 (3764565837.em) 200018 (3764565837.em) 200018 (3764565837.em) 200018 (3764565837.em) 200018 (37645658.em) 200019 (37645658.em) 200019 (37645658.em) 200019 (376456387.em) 200019 (37647668387.em) 200019 (376476683714.em) 200019 (376476683714.em) 200019 (376476683714.em) 200019 (3764766832.em)	♥ (■♥) Sudmit Time 4/25/2013 10. 4/26/2013 12. 5/1/2013 11 5/1/2013 11 5/3/2013 72 4/25/2013 12 4/25/2013 12 5/3/2013 72 5/3/2013 72 4/25/2013 12 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 4/25/2013 10 5/3/2013 72 5/3/2013 72 5/	Display Time Zone Subject Find Find Copplay Time Zone Subject Find Fi	2 Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win8@live.com> Peter Vilson opeterwils
Email Rems		Name 200014 19874 200014 19874 200014 19874 200014 19874 2000150 144136 2000162 29872 2000163 29872 2000164 19874 2000165 20872 2000164 278754 2000195 25845 2000196 278745 2000196 278745 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 278724 2000196 <t< td=""><td>♥ ₩ √ Submit Time 4/25/2013 10 4/25/2013 12 5/1/2013 11 5/3/2013 72 4/25/2013 12 5/3/2013 72 5/3/2013 72 5/3/</td><td>Display Time Zone Soliter: Pri: 04/25/2013 Daily Enal Re: 05/25/2013 Daily Enal Re: 05/25/2013 Daily Enal Re: 05/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Condy Enal</td><td>2 Eastern Daylight Time ("from local machine)</td></t<>	♥ ₩ √ Submit Time 4/25/2013 10 4/25/2013 12 5/1/2013 11 5/3/2013 72 4/25/2013 12 5/3/2013 72 5/3/2013 72 5/3/	Display Time Zone Soliter: Pri: 04/25/2013 Daily Enal Re: 05/25/2013 Daily Enal Re: 05/25/2013 Daily Enal Re: 05/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Condy Enal	2 Eastern Daylight Time ("from local machine)
Tena Items 1 Image: Status 1 <		Name 2000014 158-67 2000014 158-67 200014 158-67 200014 158-67 200014 158-67 200014 158-67 200014 158-67 200015 256-56 200016 256-56 200016 256-56 200016 256-56 200016 256-57 200016 156-56 200016 156-56 200016 156-56 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57 200016 156-57	♥ ₩ ₩ Submt Tme 4/25/2013 10. 4/25/2013 12. 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 12 4/25/2013 12 4/25/2013 12 4/25/2013 12 4/25/2013 10 4/25/2013 10 5/1/2013 10 4/25/2013 10 4/25/2013 10 5/1/2013 1	Enal Display Time Zone Subject Enal Display Enal E	2 Eastern Daylght Time (From local machine) Eastern Daylght Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics of PeterWilson.Win7@pmat Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics of PeterWilson.Win7@pmat Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics of PeterWilson.Win7@pmat Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics of PeterWilson.Win7@live.com> Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics of PeterWilson.Win7@live.com> Peter Wilson opeterWilson.Win7@live.com> WindowsSeven Forensics
■ Enail Remis 1 ■ Enail Remis 1 ■ Enail Remis 1 ■ Enail Actives 1		Name 200014 (1) 49574 (4) 45874 (4) 45874 (4) 45874 (4) 45874 (4) 45874 (4) 45874 (4) 41 4) 41 4 4) 41 4 4) 41 4 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4 4) 41 4)	♥ (₩) (¥25/2013 10 4/25/2013 12 4/25/2013 12 5/1/2013 11 5/1/2013 11 5/3/2013 72 4/25/2013 12 5/3/2013 72 5/3/2013 10 4/2/3/2013 10 5/4/2013 34	Display Time Zone Soliter: Pri: 04/25/2013 Daily Enal Re: 04/26/2013 Daily Enal Ot/2/2013 Daily Enal Ot/26/2013 Daily Enal Ot	s Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@kve.com> Peter Wilson opeterwilson.win8@kve.com> MindowsSeven Foreacid. effectWilson.Win7@pmat Peter Wilson opeterwilson.win8@kve.com> WindowsSeven Foreacid. effectWilson.Win7@pmat Peter Wilson opeterwilson.win8@kve.com> WindowsSeven Foreacid. effectWilson.Win7@pmat Peter Wilson opeterwilson.wi
Tena Items 1 Image: Status		Name Name 2000014 1989-9496-b521a.em 200014 1987-1bd/387d.em 200015 2167-357-1bd/387d.em 200016 2167-357-356.em 200016 2167-357-356.em 2000116 2167-357-367.em 2000116 2167-357.em 2000116 2167-378.em 2000117 2167-467.em 2000116 2168-358.em 20000116 2168-358.em 20000116 2168-358.em 20000116 2168-358.em 20000116 2168-358.em 20000116 216	the state of	Complex Time 2 and C	Estern Daylght Time (From local machine) Estern Daylght Time (From local machine) Peter Wison opeterwison.win8@kv.ccm> Wison opeterwison.win8@kv.ccm> Vison opeterwison.wisol@kv.ccm> Vison opeterwis
Enal Rens 1 Image: Constraint and the set of		Name 200014 (1) 49574 (1) Lasting 200014 (1) 49574 (1) Lasting 200014 (1) 49574 (1) Lasting 200016 (2) 50574 (2) Lasting 200016 (2) 50576 (2) Lasting 200017 (2) 50576 (2) Lasting 200018 (2) 50576 (2) Lasting 200018 (2) 50576 (2) Lasting <td></td> <td>Display Time Zone Solicited Fiv: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Complete Complete Enal Complete Complete Enal Complete Complete Enal Complete Enal Complete Complete Complete Complete Enal Complete Com</td> <td>Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics cPeterWilson.Win7@lignam Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensiscs cPeterWilson</td>		Display Time Zone Solicited Fiv: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Complete Complete Enal Complete Complete Enal Complete Complete Enal Complete Enal Complete Complete Complete Complete Enal Complete Com	Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensics cPeterWilson.Win7@lignam Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensiscs cPeterWilson
Enail Items 1 Imail Items<		Hame 2000014 1989-9496-b521a.em 200014 1987-1bd/387d.em 200016 1987-1bd/387d.em 200016 2987-1bd/387d.em 200016 2987-1bd/387d.em 200016 2987-1bd/387d.em 200016 2086-2886-713-658-65 200016 2987-49867.em 200016 2498-2886-714-867-714 200016 2498-714-867-714-86 200016 2498-714-867-714-86 200017 2578-714-867-86 2000018 2578-714-82-86 2000018 2578-714-82-86 2000018 258-714-82-86 2000018 258-714-82-86 2000018 258-714-82-86 2000018 258-714-82-81 2000018 258-787-7130-86 2000018 258-787-7130-86 200018 258-787-7130-86 200018 258-787-780-87 200018 258-787-780-87 200018 258-787-780-87 200018 258-787-780-87 200018 258-787-780-87	• ₩•• Submit Time 4[25](2013 10 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 12 4[26](2013 10 4[26](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10 4[28](2013 10	Copyley Time Zone Copyley Time Copyley T	st Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensic cPeterWilson.Win7@gmal Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forensic cPeterWil
Enail Items 1 Imail Items<		Name 200014 c. 1987; hbd587 am 200014 c. 1987; hbd587 am 200014 c. 1987; hbd587 am 200015 j. d443 as15 as21 f. em 200016 j. 2987; hbd587 am 200016 j. 9587; hbd587; hbd78; hbd787; hbd787		Display Time Zone Solicit First 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal Oldy Enal Oldy/Enal Oldy/	s Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) To Peter Wison opeterwison.win8@kve.com> Wison opeterwison.win8@kve.com
Enail Items 1 ■ Enail Struce ■ Enail Struce ■ Enail Voltes ■ Enail Addresses ■ Enail Addresses ■ Continn+copyCalpsavcb24uc50uc6bohf ■ Continn+copyCalpsavcb24uc50uc6bohf ■ Continn+copyCalpsavcb24uc50uc6bohf ■ Continn+copyCalpsavcb24uc50uc6bohf ■ Content-secutiv+norephyBaccourt.micross ■ Content-secutiv+norephyBaccourt.micross ■ Content-secutiv+norephyBaccourt.micross ■ Content-secutiv+norephyBaccourt.micross ■ Content-secutiv+norephyBaccourt.micross ■ Content-secutiv+norephyBaccourt.micross ■ Content-secutiv-norephyBaccourt.micross ■ Content-secutiv-norephyBaccourt.micross ■ Content-secutiv-model ■ Content-secutiv-model ■ Content-secutiv-model <tr< td=""><td>> -</td><td>Hame 2000014 1989/971bd38874 2000014 1989/971bd38874 2000116 1987/71bd38874 2000116 2786/71bd38874 2000116 2786/751 2000116 2786/751 2000116 2786/751 2000116 2786/751 2000116 2786/751 2000116 2486/8586/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 20000116 1566/751 20000116 1566/751 20000116 1566/751 20000116 1566/751 20000116 1566/756 20000116 1566/756 20000116 1566/756 <</td><td>● ● Submit Time 4/25/2013 10. 4/25/2013 12. 4/25/2013 12. 5/1/2013 11 5/1/2013 11 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 <</td><td>Email Dopkey Time Zone Sobject Free 04/25/2013 Daty Email Re: 04/25/2013 Daty Email Free 04/25/2013 Daty Email Fre: 04/25/2013 Daty Email O4/25/2013 Daty Email 04/25/2013 Daty Email O4/25/2013 Daty Email</td><td>Estern Daylght Time (From local machine) Estern Daylght Time (From local machine) Peter Wison opeterwison.win8@live.com> WindowsSeven Forencis cPeterWison.Win7@gmal Peter Wison opeterwison.win8@live.com> WindowsSeven Forencis cPeterWison.Win7@gmal.com> WindowsSevenF</td></tr<>	> -	Hame 2000014 1989/971bd38874 2000014 1989/971bd38874 2000116 1987/71bd38874 2000116 2786/71bd38874 2000116 2786/751 2000116 2786/751 2000116 2786/751 2000116 2786/751 2000116 2786/751 2000116 2486/8586/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 2000116 1566/751 20000116 1566/751 20000116 1566/751 20000116 1566/751 20000116 1566/751 20000116 1566/756 20000116 1566/756 20000116 1566/756 <	● ● Submit Time 4/25/2013 10. 4/25/2013 12. 4/25/2013 12. 5/1/2013 11 5/1/2013 11 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 4/23/2013 10 <	Email Dopkey Time Zone Sobject Free 04/25/2013 Daty Email Re: 04/25/2013 Daty Email Free 04/25/2013 Daty Email Fre: 04/25/2013 Daty Email O4/25/2013 Daty Email	Estern Daylght Time (From local machine) Estern Daylght Time (From local machine) Peter Wison opeterwison.win8@live.com> WindowsSeven Forencis cPeterWison.Win7@gmal Peter Wison opeterwison.win8@live.com> WindowsSeven Forencis cPeterWison.Win7@gmal.com> WindowsSevenF
Enail Items 1 Imail Items </td <td>> 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0</td> <td>Variantic Variantic Variantic Variantic 200014 1987-01405473 and 200014 1987-01405473 and 200015 1947-34515461 fam 200016 2546-252-853. and 200016 2546-252-853. and 200016 2546-252-853. and 200016 2546-252-874. and 200016 4555-2677. and 200016 4565-2647-4863. and 200017 4565-2647-2863. and 200018 5-2647-2863. and 200018 5-2648-2863. and 200018 5-2648-2863. and 200018 5-2647-2863. and 200018 5-2648-2864. and 200018 5-2644-2863. and 200018 5-2644-2864. and <</td> <td>● ● Submit Time 4/25/2013 10. 4/25/2013 10. 4/26/2013 12. 4/26/2013 12. 4/26/2013 12. 5/1/2013 11 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72</td> <td>Dopkey Time Zone Sobiect First 94/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 05/21/2013 Daily Enal Re: 05/21/2013 Daily Enal Re: 05/21/2013 Daily Enal First 94/25/2013 Daily Enal Configure Solution Solution First 94/25/2013 Daily Enal Configure Solution Configure Solution Solution Configure Solution Solution Configure Solution Configure Solution Solution Configure Solution Solution Configure Solution Configure Solution Solu</td> <td>Eastern Daylight Time (from local machine) Eastern Daylight Time (from local machine) To Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forenacs CelterWilson.Win7@opma Peter Wilson opeterwilson.win8@</td>	> 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0	Variantic Variantic Variantic Variantic 200014 1987-01405473 and 200014 1987-01405473 and 200015 1947-34515461 fam 200016 2546-252-853. and 200016 2546-252-853. and 200016 2546-252-853. and 200016 2546-252-874. and 200016 4555-2677. and 200016 4565-2647-4863. and 200017 4565-2647-2863. and 200018 5-2647-2863. and 200018 5-2648-2863. and 200018 5-2648-2863. and 200018 5-2647-2863. and 200018 5-2648-2864. and 200018 5-2644-2863. and 200018 5-2644-2864. and <	● ● Submit Time 4/25/2013 10. 4/25/2013 10. 4/26/2013 12. 4/26/2013 12. 4/26/2013 12. 5/1/2013 11 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72. 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72 5/3/2013 72	Dopkey Time Zone Sobiect First 94/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 05/21/2013 Daily Enal Re: 05/21/2013 Daily Enal Re: 05/21/2013 Daily Enal First 94/25/2013 Daily Enal Configure Solution Solution First 94/25/2013 Daily Enal Configure Solution Configure Solution Solution Configure Solution Solution Configure Solution Configure Solution Solution Configure Solution Solution Configure Solution Configure Solution Solu	Eastern Daylight Time (from local machine) Eastern Daylight Time (from local machine) To Peter Wilson opeterwilson.win8@live.com> WindowsSeven Forenacs CelterWilson.Win7@opma Peter Wilson opeterwilson.win8@
Enal Rens I 6 Find Status 6 Enal Actives 7 Enal Actives		Name 2000014 1,985949486521a.em 2000014 1,98571bdd3887d.em 200016 1,98571bdd387d.em 200016 2,98571bdd3887d.em 200016 2,78571bd3887d.em 200016 2,78571bd3887d.em 200016 2,785745355464.em 200016 2,785745355464.em 200016 2,78574535744867.em 2000016 4,9787453571423.em 2000016 2,787453571423.em 2000016 2,7874555671423.em 2000016 2,537564735.em 2000015 2,537578645.em	♦ (##) \$\$\$ \$\$\$ \$\$\$\$ \$	Display Time Zone Solicit Fiv: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Fiv: 04/25/2013 Daily Enal fie: 04/25/2013 Daily Enal	Extern Daylight Time (From local machine) Image: Comparison of the second of the s
Tenai Rens 1 Imail Rens 1 Imail Podre 1		Vene 200014 (1) 9874 (4) 9876 9486521 a.m. 200014 (2) 9874 (1) 45874 a.m. 200015 (2) 7475 (5) 45874 a.m. 200016 (2) 9875 (2) 7475 (5) 45874 a.m. 200016 (2) 9875 (2) 74874 a.m. 200016 (2) 9875 (2) 74874 a.m. 200016 (2) 9875 (2) 74874 a.m. 200016 (2) 7475 (2) 74874 a.m. 200016 (2) 7475 (2) 74874 a.m. 200016 (2) 7475 (2) 74835.0 m. 200016 (2) 7475 (2) 74835.0 m. 2000016 (2) 7475 (2) 7475 (2) 7475.0 m. 2000016 (2) 7475 (2) 7475.0 m. 2000016 (2) 7475 (2) 7475.0 m. 2000016 (2) 7475 (2) 7475.0 m. 2000015 (2) 7475 (2) 7475.0 m.	▼ ●●● Submit Time 4/25/2013 12 4/26/2013 12 4/26/2013 12 5/1/2013 11 5/3/2013 72 4/23/2013 34 4/23/2013 34 4/23/2013 4 4/23/2013 4	Display Time Zone Soliter: First 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal Ord/27/2013 Daily Enal	Eastern Daylight Time (From local machine) Eastern Daylight Time (From local machine) ▲ To Peter Wilson opeterwilson.win8@kvn.ccm> Peter Wilson opeterwilson.win8@kvn.ccm> WindowsSeven Forensis of PeterWilson.Win7@gma Peter Wilson opeterwilson.win8@kvn.ccm>, WindowsSeven Forensis of PeterWilson.Win7@gma WindowsSeven Forensis of PeterWilson.Win7@gmaLcm>, WindowsSeven Forensis of PeterWilson.Win7@gma WindowsSeven Forensis
Tenai Rens 1 Imail Rens 1 Imail Podre 1		Vene 200014 - (JSS-7bd3854; en 200014 - (JSS-7bd386; en 200014 - (JSS-7bd386; en 200014 - (JSS-7bd386; en 200015 - (JSS-7bd386; en 200015 - (JSS-7bd386; en 200015 - (JSS-7bd386; en 200015 - JSS-3b136577e-5; en	♥ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Display Time Zone Soliter: First 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal Other 04/25/2013 Daily	Extern Daylight Time (From local machine) Image: Comparison of the second of the s
Tend Items 1 H ■ End Status H ■ End Actives H = End Actives		Name 200014 19870 200014 19870 200014 19870 200014 19870 200014 19870 2000150 194734515421 2000161 2967222535 2000162 2966222535 2000162 2966225355 2000163 1967243353 2000164 5975435356 2000164 5975435339 2000164 5975435339 2000164 5975435339 2000164 595543539 2000164 5975435339 2000164 5975435339 2000164 5975435339 2000164 5975435339 2000164 5975435339 2000164 5975435339 2000165 5337596714033 2000164 5973453339 2000165 533135637345339	▶ ##+ Submit Time 4/25/2013 10 4/26/2013 12 4/26/2013 12 5/1/2013 11 5/3/2013 72 5/3/2013 72 5/3	Display Time Zone Soliter: First 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal Ret 04/25/2013 Daily Enal First 04/25/2013 Daily Enal Ody/Enal Ody/Enal Ody/Enal Ody/Enal Ody/25/2013 Daily Enal Ody/Enal Ody/25/2013 Daily Enal O	Estern Daylight Time (From local machine) Estern Daylight Time (From local machine) ► To Peter Wilson cpetertwilson.win88jkvn.com> Peter Wilson cpeterwilson.win88jkvn.com> Peter Wilson cpeterwilson.win88jkvn.com> WindowsSeven Forensis cPeterWilson.Win78jgma Peter Wilson cpeterwilson.win88jkvn.com> WindowsSeven Forensis cPeterWilson.Win78jgmal.com> WindowsSeven
Enail Rens Form (147)		Varia Varia Varia Varia 200014 1987-1045574 onl 200015 1987-1045574 onl 200016 1987-1045574 onl 200016 1987-1045574 onl 200016 2987-1045574 onl 200016 2987-1045574 onl 200016 2987-1045574 onl 200016 4987-1045574 onl 200016 4987-1045574 onl 200016 4987-1045574 onl 200016 4987-104574-1045574 onl 200016 4987-104574-1045574 onl 200017 4987-104574-1045574 onl 200017 4987-104574-1045780-0 200017 4987-104574-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-1045780-0 200017 4987-104	▶ ##+ Submit Time 4/25/2013 10., 4/26/2013 12., 4/26/2013 12., 5/1/2013 11 5/3/2013 72 5/3/2013 72	Display Time Zone Solicient First 04/25/2013 Daily Email Ret: 04/25/2013 Daily Email Ret: 04/25/2013 Daily Email Ret: 04/25/2013 Daily Email Ret: 05/25/2013 Daily Email Ret: 05/25/2013 Daily Email First: 04/25/2013 Daily Email Control Daily Email	Estern Daylght Time (from local machine) Estern Daylght Time (from local machine) Peter Wilson opeterwilson.win8@kw.c.com> Peter Wilson opeterwilson.win8@kw.c.com> WindowsSeven Forensics oPeterWilson.Win7@gmail Peter Wilson opeterwilson.win8@kw.c.com>, WindowsSeven Forensics oPeterWilson.Win7@gmail Peter Wilson opeterwilson.win8@kw.c.com>, WindowsSeven Forensics oPeterWilson.Win7@gmail Peter Wilson opeterwilson.win8@kw.c.com>, WindowsSeven Forensics oPeterWilson.Win7@gmail MendowsSeven Forensics oPeterWilson.Win7@gmail.com> WindowsSeven Forensics oPeterWilson.Win7@gmail.com>, WindowsSeven Forensics oPeterWilson.W
Enal Rens Form (IS Status Form		Value Name 200014 1,987-948-b52.1.a.mf 200014 1,987-948-b52.1.a.mf 200014 1,987-948-b52.1.a.mf 200014 1,987-948-b52.1.a.mf 200015 1,643-645-84-8.mf 200016 2,646-6226-258-56-mf 200016 2,646-6226-258-56-mf 200016 2,646-6226-258-56-mf 200016 4,556-56-56-66-mf 200016 4,556-56-56-66-mf 200016 4,556-56-56-66-mf 200016 4,556-56-56-66-mf 200016 4,556-56-76-76-56-66-mf 200016 4,556-56-77-46-76-56-66-mf 200016 4,556-56-77-46-76-56-66-mf 200016 4,556-56-77-46-76-56-67-mf 200016 4,556-56-77-46-76-56-67-mf 200016 5,537-78-56-67-mf 200016 5,537-78-56-67-mf 200016 5,537-78-56-67-mf	■ ##= Submit Time 4/25/2013 10. 4/26/2013 12. 4/26/2013 12. 5/1/2013 11 5/3/2013 72 5/3/2013 72 4/23/2013 10 4/23/2013 4 4/23/2013 4	Display Time Zone Solicit First 94/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 04/25/2013 Daily Enal Re: 050/2013 Daily Enal Re: 050/2013 Daily Enal Re: 050/2013 Daily Enal Re: 050/2013 Daily Enal First 94/26/2013 Daily Enal Re: 050/2013 Daily Enal Re: 050/2013 Daily Enal First 94/26/2013 Daily Enal First 94/26/2013 Daily Enal First 94/26/2013 Daily Enal Comparison First 94/26/2013 Daily Enal First 94/26/2013 Daily Enal Comparison Comparison First 94/26/2013 Daily Enal Comparison First 94/26/2013 Daily Enal Comparison Compar	Extern Dwjolpt Time (from local machine) Image: Comparison of the state of t
mail tens 1 b fmill tens c fmill tens		Varianti Varianti Varianti Varianti 200014: 1987:104584 200014: 1987:104584 200014: 1987:104584 200015: 10453:10454 200016: 2767:65584 200016: 10456:1584:1 200016: 10456:1584:1 200016: 10456:1584:1 200016: 10456:1584:1 200016: 10456:1584:1 200016: 10456:1584:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1 200016: 10456:1484:1	(₩) (₩)	Display Time Zone Solied: Even 04/25/2013 Daly Enal Fer 04/25/2013 Daly Enal Fer 04/25/2013 Daly Enal Fer 04/25/2013 Daly Enal Fer 05/25/2013 Daly Enal Of/25/2013 Daly Enal O	Extern Daylght Time (from local machine)
Ten al tens 1 0 - final status 0 - final Actives 0 - final Active </td <td></td> <td>Image 200014 (1)987-108458 (a) 200014 (1)987-108458 (a) 200015 (2)4743-513645 (a) 200016 (2)4743-513645 (a) 200017 (2)4743-513645 (a) 200013 (2)4744-735645 (a) 200013 (2)4744-7356458 (a) 200013 (2)4744-735658 (a) 200013 (2)4744-735658 (a) 200013 (2)4744-735658 (a) 200013 (2)4744-73568 (a) 200013 (2)4744-73568 (a) 200013 (2)4756-7378-7588 (a) 200013 (2)475688 (a) <</td> <td>(₩) (₩)</td> <td>Display Time Zone Solie Display Email Display Time Zone Display Email First 04/25/2013 Daly Email Of/25/2013 Daly Email Of/25/201</td> <td>Eatern Daylght Time (from local machine) E tatern Daylght Time (from local machine) To Peter Wison opeterwison.win8@kw.com> Wison opeterwison.win8@kw.com> Peter Wison opeterwison.win8@kw.com> Peter Wison opeterwison.win8@kw.com> Wison opeterwison</td>		Image 200014 (1)987-108458 (a) 200014 (1)987-108458 (a) 200015 (2)4743-513645 (a) 200016 (2)4743-513645 (a) 200017 (2)4743-513645 (a) 200013 (2)4744-735645 (a) 200013 (2)4744-7356458 (a) 200013 (2)4744-735658 (a) 200013 (2)4744-735658 (a) 200013 (2)4744-735658 (a) 200013 (2)4744-73568 (a) 200013 (2)4744-73568 (a) 200013 (2)4756-7378-7588 (a) 200013 (2)475688 (a) <	(₩) (₩)	Display Time Zone Solie Display Email Display Time Zone Display Email First 04/25/2013 Daly Email Of/25/2013 Daly Email Of/25/201	Eatern Daylght Time (from local machine) E tatern Daylght Time (from local machine) To Peter Wison opeterwison.win8@kw.com> Wison opeterwison.win8@kw.com> Peter Wison opeterwison.win8@kw.com> Peter Wison opeterwison.win8@kw.com> Wison opeterwison

	Explore Overview Email Graphics Bookmarks Live Sev	arch Index	x Search Volatile				4 Þ
	Creat Range (A.N.	Fie List					
	The Fred Calu	- 80	a 🖊 🚼 🔳	•	🗂 📄 🥅 Email 🗸 Display Time Zoni	: Eastern Daylight Time (From local machine)	😸 🦽 🗙 🗧
	H-Se Email Status		Name	Submit Time	Subject	▲ T0	
	Email by Date		2000015e 542804b61d2cc2.eml	5/1/2013 11:	05/01/2013 Daily Email with Text and Picture Attachments	"PeterWilson, Win8@gmail.com" <peterwilson, td="" win8@gma<=""><td>il.com>, WindowsSeven Forensics <peter< td=""></peter<></td></peterwilson,>	il.com>, WindowsSeven Forensics <peter< td=""></peter<>
	E- Tail Addresses		2000015f_2f0f7032744f6.eml	5/1/2013 11:	05/01/2013 Daily Email with Text and Picture Attachments	"PeterWilson.Win8@gmail.com" <peterwilson.win8@gma< th=""><th>il.com>, WindowsSeven Forensics <peter< th=""></peter<></th></peterwilson.win8@gma<>	il.com>, WindowsSeven Forensics <peter< th=""></peter<>
	😑 🖾 Senders [From] (87 / 87)		20000148_fb3a4a17d5292.eml	4/26/2013 11	04/26/2013 Daily Email	Windows8 Gmail <peterwilson.win8@gmail.com>, Peter</peterwilson.win8@gmail.com>	Wilson <peterwilson.win8@live.com>, V</peterwilson.win8@live.com>
	Email Domains [11 / 11]		20000149_8b414805342d3c.eml	4/26/2013 11	04/26/2013 Daily Email	Windows8 Gmail <peterwilson.win8@gmail.com>, Peter</peterwilson.win8@gmail.com>	Wilson <peterwilson.win8@live.com>, W</peterwilson.win8@live.com>
	E Carl Display Name (87/87)		2000014a_451e528741b578.eml	4/26/2013 11	04/26/2013 Daily Email	Windows8 Gmail <peterwilson.win8@gmail.com>, Peter</peterwilson.win8@gmail.com>	Wilson <peterwilson.win8@live.com>, V</peterwilson.win8@live.com>
	- account-security-noreply@account.microsof	a 🗆 🖂	2000007f_649d4756b23014.eml	4/21/2013 4:	04/21/2013 Daily Email	Windows8 Gmail <peterwilson.win8@gmail.com>, Windo</peterwilson.win8@gmail.com>	wsSeven Forensics <peterwilson.win7@l< th=""></peterwilson.win7@l<>
	🔚 confirm+acgv0zxj3awxzb24ud2luoebnbwfpt	د H	20000108_c000c2c2f2bd1_cml	4/21/2013 4:	04/21/2013 Daily Email 05/02/2013 Daily Email	Windows8 Gmail <peterwilson.win8@gmail.com>, Windo WindowsSouce Ecceptics <deterwilson win7@lue.com=""></deterwilson></peterwilson.win8@gmail.com>	"Deterfulces Win9@amail.com" (Deterful
	Connect@windowslivemail.com(3/3)		20000190_69990280/2001.em	5/3/2013 5:0	05/03/2013 Daily Email	WindowsSeven Forencics <peter com="" wilson,="" win="" wive,=""></peter>	"Deteriwison Win9@mail.com" <detervi< th=""></detervi<>
	- Internetexplorer@email2.microsoft.com (1/	163	20000137 a7010e76a406b2.eml	4/24/2013 9:	04/24/2013 Email with Attachment	WindowsSeven Forensics <peterwilson.win7@live.com></peterwilson.win7@live.com>	WindowsSeven Forensics <peterwilson.< th=""></peterwilson.<>
	mail-norepiy@google.com(3/3)		20000138_698e2ec6d1774f.eml	4/24/2013 9:	04/24/2013 Email with Attachment	WindowsSeven Forensics <peterwilson.win7@live.com></peterwilson.win7@live.com>	WindowsSeven Forensics <peterwilson.< th=""></peterwilson.<>
	- Incrareivyfba.iva8=vvir.obz-c7978@postm	1ē					
	🔚 noreply-475ba29f@plus.google.com (2 / 2))					
	— Call noreply-daa26fef@plus.google.com (1/1))					
	Inotification+z)4yzya_=_c@facebookmail.co	x					
	Deterwision.win/@gmail.com(10/10)						
	peterwilson.win8@gmail.com (23 / 23)						
	peterwilson.win8@live.com(11/11)						
	🔚 pjw5578@rit.edu (2 / 2)						
	-Call update+zj4yzya_=_c@facebookmail.com ((
	- Cell windows@email.microsoft.com (1/1)						
	Windowsig/email2.microsort.com (3/3)						
		_ بر ا					T.
		Loaded	11 Eftered: 11	Total: 11	Highlighted: 0 Checked: 0 Tota	1 Sizer 25 62 KB	
		- J coddou.	11 11 11 10 10 11	1 local 11	prignighted. o perioded. o proce	E3465, 23,02 ND	
		T 2	01 E		4 f		
		- F IŞ	gure 82 Em	an sen	it from peterwilson.wi	na@nve.com	
	FTK found a total (of 8	emails that y	vere fo	orwards of previously se	ent emails. In all of the	emails the receiver
	I III Iouna a total o	010	cilians that v		i wards of previously s	on emans. In an or me	emans, the receiver
was	peterwilson.win8@live	.com	n:				
	*		-				
	Evolute Overview Email Graphics Bookmarks Live Se	arch Inde	y Search Volatile				d b
		cile 100	K Dearch Voldale				4.12
	Email Items	File List					
	· · · · · · · · · · · · · · · · · · ·				Licolay line (op	e: Eastern Davlight Time. (Erom local machine)	and 10 10 10 10
	문-월 Email Status		8 🖊 📙 🔳	• •	💼 🔲 Email 🗸 Display Time Zon	e: Eastern Daylight Time (From local machine)	😻 🧖 X 🔿
	Email Status		Ame	v ∰• Submit Time	Subject	e: Eastern Daylight Time (From local machine)	From CC
	Email Status Email Attachments (36 / 36) Email Related Items (From Email) (312 / 312)		Name 20000144_d889e948eb621a.eml		Email Email Usplay Inne Zon Subject Fw: 04/25/2013 Daily Email	e: Eastern Daylight Time (From local machine) To Peter Wilson <peterwilson.win@@live.com></peterwilson.win@@live.com>	From CC <pre>cpeterwilson.win8@gmail.com></pre>
	Email Status Email Ratachments (36/36) Email Related Items (From Email) (312/312) Email Related Items (From Email) (312/312) Email Related Items (6/6)		Image: State		Image: State	Eastern Daylight Time (From local machine) To Peter Wilson <peterwilson.win8@live.com> Peter Wilson <peterwilson.win8@live.com> Peter Wilson <peterwilson.win8@live.com></peterwilson.win8@live.com></peterwilson.win8@live.com></peterwilson.win8@live.com>	From CC cpeterwilson.win0@gmail.com> cpeterwilson.win0@gmail.com> cpeterwilson.win0@gmail.com>
	Email Status Gard Status Email Attachments (36 / 36) Gard Related Items (From Email) (312 / 312) Email Repty (7 / 7) Growerdde Email (8 / 8) Email Repty (7 / 7) Growerdde Email (8 / 8)		Image: State		Comparing the second seco	Eastern Daylight Time (From local machine) To Peter Wilson cpeterwilson.win8@ilve.com> Peter Wilson cpeterwilson.win8@ilve.com> Ns Peter Wilson cpeterwilson.win8@ilve.com> Peter Wilson cpeterwilson.win8@ilve.com> Peter Wilson cpeterwilson.win8@ilve.com>	From CC cpeterwison.win0@gmail.com> cpeterwison.win0@gmail.com> cpeterwison.win0@gmail.com> cpeterwison.win0@gmail.com>
	E → End Status End Status End Status End Status End Status End Redded Itens (Fron End) (312 / 312) End Redded Itens (Fron End) (312 / 312) End Redde (7 / 7) End Redde (7 / 7) End Verbres End Verbres End Verbres		Name 20000144_d889e948eb621a.em 20000150_fd443e615a6c1f.em 20000165_2d06e22835a5b.em 2000019f_e2bdf4bec38fa4.em 20000143_dfabe1aec0b20.em	 Submit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 7:2 4/25/2013 10 	Image: Control of the second	Eastern Daylight Time (From local machine) To Organization (Peter Wilson <pre>cmo> Peter Wilson <pre>cmo> Peter</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>	Prom CC Cc cpeterwlson.win8@gmail.com> cpeterwlson.win8@gmail.com> cpeterwlson.win8@gmail.com> cpeterwlson.win8@gmail.com> cpeterwlson.win8@gmail.com>
	Email Status Email Status Email Attachments (36 / 36) Email Related Tensi (From Email) (312 / 312) Email Related Tensi (6 / 30) Email Related Tensi (36 / 30) Email Relative (7 / 7) </td <td></td> <td>Name 2000014_d899948eb621a.eml 20000150_fd443a615a8c1f.eml 20000155_2d06e228235a5b.eml 20000145_2d06e228235a5b.eml 20000145_e2bdf4bec38fa4.eml 20000143_e2bdf4bec38fa4.eml</td> <td> Eubmit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 7:2 4/25/2013 10 4/26/2013 12 </td> <td>Image: The second sec</td> <td>Estaten Daylght Time (From local machine) To Peter Wison cpeterwison.win8@Wre.com> Peter Wison cpeterwison.win8@Wre.com></td> <td>Prom CC speterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com></td>		Name 2000014_d899948eb621a.eml 20000150_fd443a615a8c1f.eml 20000155_2d06e228235a5b.eml 20000145_2d06e228235a5b.eml 20000145_e2bdf4bec38fa4.eml 20000143_e2bdf4bec38fa4.eml	 Eubmit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 7:2 4/25/2013 10 4/26/2013 12 	Image: The second sec	Estaten Daylght Time (From local machine) To Peter Wison cpeterwison.win8@Wre.com>	Prom CC speterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com>
	□ Email Relation □ Email Related Items (36 / 36) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (56 / 67 / 67) □ Email Related Items (56 / 67 / 67)		Name 20001144_d899e948eb621a.eml 2000150_fd443e615a8c1f.eml 2000156_c202622825s5b.eml 20001154_c20de622825s5b.eml 20001154_c20de622825s5b.eml 20001154_ffb5e952491667.eml 20000164_ff1eb5552e072.eml	 Eubmit Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 4/25/2013 7:2 4/25/2013 10 4/26/2013 12 5/1/2013 11 		E Eastern Daylight Time (From local machine) ▲ To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson	Prom CC opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com>
	Email Status Email Status Email Attachments (36/36) Email Redevid Lense (From Email) (312/312) Email Redevid (7/7) Email Redevid Const (3/8)		Name 2000114, d899948eb621.a.en/ 2000150, fd413a615a6c1f.em/ 2000155, 2d06e22823545.em/ 2000114; c2bde1aectb20.em/ 2000114; fb5e952494367.em/ 20001164, cff1e0552e072.em/ 20001164, cff1e0552e072.em/ 20001169, cf7923f9a2330.em/	Submit Time 4/25/2013 10 4/26/2013 11 5/1/2013 11 4/26/2013 10 4/25/2013 10 4/26/2013 11 5/1/2013 11 5/3/2013 7:2	Enal Usplay Time Zon Subject Fwv 04/25/2013 Daly Enal Fwv 04/25/2013 Daly Enal Fwv 05/02/013 Daly Enal Fwv 05/02/013 Daly Enal Fwv 05/02/013 Daly Enal Fwv 04/25/2013 Daly Enal Fwv 04/25/2013 Daly Enal Fwv 05/01/2013 Daly Enal Fwv 05/01/2013 Daly Enal	E Battern Daylight Time (From local machine) To To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson	From CC opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com> opterwison.win8@gmai.com>
	Email Status Email Status Email Attachments (36 / 36) Email Reduct Zense (From Email) (312 / 312) Email Reduct Zense (7 / 7) Email Reduct Zense (5 / 6) Email (8 / 7 / 8)		Name 20000144, d899e948ebb21a, eml 20000150, fd443a61588clf, eml 20000150, fd443a61588clf, eml 20000152, 2d042e223535b, eml 20000154, 2d042e22353552, eml 20000154, 2d042e2235352, eml 20000156, c8792379a283c0, eml	▼ ■ Submit Time 4/25/2013 10 4/25/2013 10 5/1/2013 11 5/1/2013 11 5/3/2013 7:2 4/25/2013 10 5/3/2013 11 5/3/2013 11 5/3/2013 11	Enal Usptay Unsptay Ime zon Subject Frev. 04/25(2013 Daly/ Enal Frev. 04/25(2013 Daly/ Enal Frev. 04/25(2013 Daly/ Enal Frev. 05(10) (2013 Daly/ Enal Frev. 05(10) (2013 Daly/ Enal Frev. 05(10) (2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal Frev. 04(25(2013 Daly/ Enal	i: Eastern Ugsright Time (From local machine) To Peter Wilson cpeterwilson.win8@Wve.com> Peter Wilson cpeterwilson.win8@Wve.	Prom CC cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com>
	□ Email Related Items (36 / 36) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ Email Related Items (From Email) (312 / 312) □ <t< td=""><td></td><td>Name 20000144, d899e948ebb21a.eml 20000150, fd443a61538c1f.eml 20000156, 2d66e22825358b.eml 20000147, ed84be23814.eml 20000147, ed84be23814.eml 20000147, ed84be23814.eml 20000147, ed84be23814.eml 20000147, ef14be25814.eml 20000148, ed84be23814.eml 20000144, ef14be552e072.eml 20000149_c87923F9ac83c0.eml</td><td>▼ ■ Submit Time 4/25/2013 10 4/25/2013 10 4/25/2013 11 5/1/2013 11 5/1/2013 11 5/2013 10 4/25/2013 10 4/25/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11</td><td>Constant Section 2014 Constant Section</td><td>E Eastern Daylight Time (From local machine) To To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson</td><td>Prom CC opterwison.win8@gmail.com> opterwison.win8@gmail</td></t<>		Name 20000144, d899e948ebb21a.eml 20000150, fd443a61538c1f.eml 20000156, 2d66e22825358b.eml 20000147, ed84be23814.eml 20000147, ed84be23814.eml 20000147, ed84be23814.eml 20000147, ed84be23814.eml 20000147, ef14be25814.eml 20000148, ed84be23814.eml 20000144, ef14be552e072.eml 20000149_c87923F9ac83c0.eml	▼ ■ Submit Time 4/25/2013 10 4/25/2013 10 4/25/2013 11 5/1/2013 11 5/1/2013 11 5/2013 10 4/25/2013 10 4/25/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11	Constant Section 2014 Constant Section	E Eastern Daylight Time (From local machine) To To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson	Prom CC opterwison.win8@gmail.com> opterwison.win8@gmail
	Email Status Email Status Email Attachments (36 / 36) Email Attachments (36 / 36) Email Reduct Items (From Email) (312 / 312) Email Reduct (7 / 7) Email Reduct C (7 / 7) Email Reduct (7 / 7) Email Reduct C (7 / 7) Email Reduct (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7) Email Reduct C (7 / 7)		Name 2000141_d895e948eb621a.em 2000156_d1645e5255ebf.em 2000165_d2645e255ebf.em 2000165_de1eb6235ebf.em 2000141_d5e5254756.em 2000145_de1e6252e072.em 2000145_de1e6525072.em 2000145_d67525475.em	▼ ■ Submit Time 4/25/2013 10 4/25/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/2013 10 4/25/2013 10 4/25/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11 5/1/2013 11	Comparing Enall Upplay Time Zon Subject Wrv 04/25/2013 Daly Enal Fwrv 04/25/2013 Daly Enal Fwrv 05/03/2013 Daly Enal	i: Eastern Ugs/gbt Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.wi	Prom CC cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com>
	Email Redus Email Reduct Items (%on Email) (312/312) Email Reduct Items (From Email) (312/312) Email Reduct Items (From Email) (312/312) Email Reduct Items (%on Email) (312/312)		Name 2000141_d899e949eb621a.eml 2000156_2d9ee2235eb.eml 2000156_2d9ee2235eb.eml 2000149_c2bd9bec3364.eml 2000149_c2bd9bec3364.eml 2000149_c2bd9bec302.eml 2000149_c4996252072.eml 2000149_c6972294967.eml	Jubrit Time 4/25/2013 10 5/3/2013 11 5/3/2013 11 5/3/2013 12 5/3/2013 12 5/3/2013 12 5/3/2013 12 5/3/2013 7:2	Compared and the second and the	E Eastern Daylight Time (From local machine) ▲ To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.	Prom CC cpeterwison.win8@gmai.com> cpeterwison.win8@gmai.com> cpeterwison.win8@gmai.com> cpeterwison.win8@gmai.com> cpeterwison.win8@gmai.com> cpeterwison.win8@gmai.com> cpeterwison.win8@gmai.com>
	Email Status Email Related Items (36 / 36) Email Related Items (From Email) (312 / 312) Email Related Items (From Email) (312 / 312) Email Related Items (70 / 7)		Name Name 20000141_d899e940e621a.emi 2000150_d493e6153e61f.emi 2000150_d493e622358b.emi 2000151_d2064e64002.emi 2000154_d5194667.emi 2000154_d5194657.emi 2000154_d5194672.emi 2000154_d5194672.emi 2000154_d5194672.emi 8 Fikered: 8	Judinik Time 4/25/2013 10 5/1/2013 11 5/3/2013 7:2 4/25/2013 10 5/1/2013 11 5/3/2013 12 5/1/2013 11 5/3/2013 7:2 Total: 8	Enal Usplay Time 20n Subject Fiv: 04/25/2013 Daly Enal Fiv: 04/25/2013 Daly Enal Fiv: 05/02/2013 Daly Enal Fiv: 05/02/2013 Daly Enal Fiv: 05/02/2013 Daly Enal Fiv: 04/25/2013 Daly Enal Fiv: 04/25/2013 Daly Enal Fiv: 04/25/2013 Daly Enal Fiv: 05/02/2013 Daly Enal Fiv: 05/02/2013 Daly Enal Fiv: 05/02/2013 Daly Enal Highlighted: 0 Checked: 0 Total	E Statem Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter opeterwilson.win8@live.com> Peter Wilson opeterwilson.win8@live.	From CC cpeterwison.win8@gma1.ccm> cpeterwison.win8@gma1.ccm> cpeterwison.win8@gma1.ccm> cpeterwison.win8@gma1.ccm> cpeterwison.win8@gma1.ccm> cpeterwison.win8@gma1.ccm> cpeterwison.win8@gma1.ccm>
	Email Status Email Status Email Attachments (36/36) Email Redot Drems (From Email) (312/312) Email Redot (7/7) Email Redot (7/7) Email Attachments (56/65) Email Redot (7/7) Email (87/87)		Name 2000141 d895e948eb421 a. emi 2000151 d645ae515ae17 f. emi 2000151 d645ae515ae07 f. emi 2000151 d645ae525e855 2000151 d645ae525e855 2000151 d645ae5269762 2000161 d6458269762 2000161 d6458269762 2000161 d6458269762 2000161 d6458269762 20001019 d68792639202 20001019 d68792639202 20001019 d68792639202 2000119 d6879263920 8 Fibered: 8	Submt Time 4/25/2013 10 4/26/2013 12 5/1/2013 11 5/3/2013 712 5/3/2013 712 5/3/2013 712 5/3/2013 712 Total: 8	Compared and the second s	E Satem Daylght Time (From local machine)	Pron CC cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com>
	Email Related Items (36/36) Email Related Items (From Email) (312/312)		Name 20000141_d899e940ebc21a.eml 20000151_d693ebc223.estb.eml 20000151_d6942ebc223.estb.eml 20000151_d6942ebc223.estb.eml 20000151_d6942ebc223.estb.eml 20000151_d6942ebc223.estb.eml 20000151_d6942ebc223.estb.eml 20000154_d6942ebc220ebc200 20000154_d6942ebc220ebc200 20000154_d6942ebc220ebc200 20000154_d6942ebc200 20000154_d6944ebc200 20000154_d6944ebc200 20000154ebc200	Submit Time //25/2013 10 //25/2013 12 //26/2013 12 //26/2013 12 //25/2013 12 //25/2013 11 //26/2013 12 //26/2013 7:2 //26/2013	Email Usplay: Time 201 Subject	E Batern Daylight Time (From local machine) ▲ To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.w	Prom CC cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com>
	Email Status Email Related Terms (36 / 36) Email Related Terms (700 mEmail) (312 / 312) Email Related Terms (70 mEmail) (312 / 312	I control to the second sec	Name Name 2000141_d899e940e621a.emi 2000151_d43se515e61f.emi 2000151_d2642e32584b.emi 2000151_d2642e4020a.emi 2000151_d2642e4020a.emi 2000151_d2642e4020a.emi 2000151_d2642e4020a.emi 8 Fikered: 8	Submit Time 4/25/2013 10 4/26/2013 12 5/3/2013 11 5/3/2013 12 5/3/2013 12 5/3/2013 12 5/3/2013 72 Total: 8 Yagure	Email Usplay: Ima 200 Subject Fixed 2003 Fixed 262013 Daly Email Fixed 262013 Daly Email Fixed 262013 Daly Email Fixed 26102 Daly Email Fixed 26102 Daly Email Fixed 26102 Daly Email Fixed 26103 Daly Email Fixed 26103 Daly Email	E Satem Daylght Time (From local machine)	From CC cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com> cpeterwison.win8@gmail.com>
	Email Robus Email Rob		Name 20000141_d889e94964621a.eml 20000150_d6892622358b.eml 20000150_d6892622358b.eml 20000150_d68926194687.eml 20000141_d5894194687.eml 20000141_d5894194687.eml 20000141_d689419465874.eml 8 Fitzened: 8		Comparing Control of Control	E Battern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@Wvs.com> Peter Wilson opeterwilson.win8@Wvs.c	Pron CC cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com> cpeterwison.win8@gmal.com>
	Final Reduct tenses (36/36) Final Reduct tense (760 m Email (312/312) Final Reduct tense (700 m Email (312/312) Final Reduct (17) Final Reduct tense (17) Final Reduct	of 7	Name Name 20001141_d899e940e6c21a.emi 20001151_d1439e515bot1.emi 20001151_d2452255b.emi 20001151_d2452255b.emi 20001151_d155256072.emi 20001151_d155256072.emi 20001151_d155256072.emi 8 Filtered: 8 F emails that v		Constant Section 2014 Constant Section	E Statem Daylght Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.win8	From CC optertwison.win8@gmal.com> optertwison.win8@gmal.com> optertwison.win8@gmal.com> optertwison.win8@gmal.com> optertwison.win8@gmal.com> optertwison.win8@gmal.com> optertwison.win8@gmal.com> typeterwison.w
	Final Status Final Status Final Status Final Status Final Regiv (777) Final Regiv (777) Final Regiv (777) Final Regiv (777) Final Regiv (777) Final Regiv (777) Final Addresses Final Addresses Final Addresses Final Regiv (7787)	of 7	Name Name 2000141_d889e940e4621a.eml 2000151_d743e615abc1f.eml 2000151_d742e62235e4b.eml 2000151_d742e62235e4b.eml 2000151_d742e62424607.eml 2000151_d742e642603.eml 2000151_d742e64244607.eml 2000154_d752e672.eml 2000154_d752e672.eml 8 Fitzered: 8 F emails that v	• •	Control C	E Batern Ugslight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Vilson opeterwilson.win	From CC optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> cpeterwison.win8@gmail.com> terterw
	FIGURE Construction of the second sec	of 7	Name 20000141_0899e940e6c21a.eml 20000150_16243e622358b.eml 20000150_2042e22358b.eml 20000150_2042e22358b.eml 20000150_2042e2358b.eml 20000150_2042e149667.eml 20000150_2042e14967.eml	(■*) (■*)	Comparison of the second	E Batern Daylght Time (from local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.win8	From CC optetrwison.win8@gmail.com> optetrwison.win8@gmail.com> mails, the receiver Image: the state stat
was	FTK found a total of either peterwilson.win7	of 7	Name Name 2000141_0899940e621a.emi 2000151_0443a613ba01f.emi 2000151_0443a613ba01f.emi 2000151_02464ac3364.emi 2000151_04164ac3061.emi 2000151_04164ac3061.emi 2000151_04164ac3061.emi 2000151_04161ac3061.emi 2000151_04161ac3061.emi 8 Fitzerd: 8 F emails that v mail.com or	\$starts Time \$starts Time \$425(2013) 12 \$\$1/2013 12 \$\$1/2013 11 <t< td=""><td>Constant of the second se</td><td>E Batern Usylght Time (From local machine) To Peter Wison opeterwison.win8@live.com> Peter Vison opetervison.win8@live.com> Peter Vison opetervison.win8@live.com> Peter Vis</td><td>From CC optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> cpeterwison.win8@gmail.com></td></t<>	Constant of the second se	E Batern Usylght Time (From local machine) To Peter Wison opeterwison.win8@live.com> Peter Vison opetervison.win8@live.com> Peter Vison opetervison.win8@live.com> Peter Vis	From CC optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> cpeterwison.win8@gmail.com>
was	Find Fabur Find Fabric Machinets (36/36) Find Redet Urins (From Enal) (312/312) Find Redet Urins Find Redet Cinal (8/8) Find Redet Find Find Redet Find	of 7	Name 20001141_d899e914964621a.eml 20001151_d699e91696621a.eml 20001151_d699e8223584b.eml 20001151_dc91648462364.eml 20001151_dc9164862364.eml 20001151_dc9164852072.eml 8 Fitered: 8 F emails that v mail.com or	\$start Time \$start Time \$425(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 310 \$1/25(20) 311 \$1/2003 31 \$1/2003 31 <td>Comparing and Development of the sense of the sense</td> <td>E Eastern Daylight Time (from local machine) To Peter Wilson opeterwilson.win8@Wvs.com> Peter Wilson opeterwilson.win8@Wvs.c</td> <td>From CC optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> translas, the receiver</td>	Comparing and Development of the sense	E Eastern Daylight Time (from local machine) To Peter Wilson opeterwilson.win8@Wvs.com> Peter Wilson opeterwilson.win8@Wvs.c	From CC optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> optertwison.win8@gmail.com> translas, the receiver
was	FIGURE Coversey Engl (Septes: Boolmarks (26/36) Final Related Items (760 Final) (312/312) Final Related Items (700 Final) (312/312) Final Related Items (300 Final) (312/312) Final Related Items	of 7	Name Name 20000141_d899e940ebc21a.eml 20000151_d615abc11.eml 20000151_d615abc12.eml 20000151_d615abc11.eml 20000151_d615bc11.eml 20000151_d615bc11.eml 20000151_d615bc11.eml 20000151_d615bc11.eml 20000151_d615bc11.eml 8 Filtered: 8 F emails that v mail.com or , search (Valation)	\$sbmt Tme \$sbmt Tme \$425(203) 10 \$1/25(203) 10 \$5/1(203) 11 \$5/1(203) 11 \$5/3(203) 7.2 \$1/25(203) 10 \$1/25(203) 10 \$1/25(203) 7.2 \$1/25(203) 7.2 \$1/25(203) 7.2 \$1/25(203) 7.2 \$1/2013 11 \$1/2013 12 \$1/2013 17 \$1/2013 17 \$1/2013 17 \$1/2013 17 \$1/2013 17 \$1/2013 17 \$1/2013 17 \$1/2013 17 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10 \$1/2014 10	Comparison of the second	E Batern Daylght Time (from local machine) ▲ To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.wi	From CC opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> mails, the receiver opeterwison.win8@gmal.com>
was	Final Status Final Status Final Attachments (36/36) Final Reddet Dense (From Email) (312/312) Final Reddet Crist Final Re	of 7	Name Name 2000141_d899e940e621a.emi 2000151_d493e915abc1f.emi 2000151_d204e2255eb.emi 2000151_d204ea4c02a.emi 2000151_d204ea4c02a.emi 2000151_d204ea4c02a.emi 2000151_d204ea4c02a.emi 2000151_d204ea4c02a.emi 8 Fikered: 8 F emaails that v mail.com or 2 Search Woldte	\$starts Time \$starts Time \$425(20) 310 \$\$1/25(20) 310 \$\$1/2013 11	Construction C	E Statem Daylght Time (From local machine) To Peter Wison opeterwison.win8@live.com> Peter Wis	From C opetertwison.win8@gmal.com> opeterwison.win8@gmal.com>
was	FTK found a total of either peterwilson.win7	of 7	Name Vision 20000141_0899e94be8c21a.eml 20000151_0493e923584b.eml 20000151_0249e822584b.eml 20000151_02494e82364.eml 20000151_02494e82364.eml 8 Fittered: 6 F emails that v mail.com or colspan="2">colspan="2" 8 Fitered: 6 F mails that v mails com or colspan="2"		Comparison of the second	E Eastern Daylight Time ("rom local machine) To Peter Wilson cpeterwilson.win8@live.com> Peter Wilson cpeterwilson.w	Image: Contract of the second of the seco
was	Final Relation of the second s	of 7	Name Viewe 20000141_d899e940e6c21a.eml 20000151_d943e623554b.eml 20000151_d943e623554b.eml 20000151_d942e623554b.eml 20000151_d942e623554b.eml 20000151_d942e632554b.eml 20000151_d942e7354283c0.eml 8 Fitered: 8 F emails that v mail.com or x5eech. Waldie x5eech. Waldie	\$sbmt Tme \$sbmt Tme \$425(23) 10 \$1/25(23	Comparison of the second	E Eastern Day/ght Time (From local machine) To Peter Wison opeterwison.win8@live.com> Peter Vison opetervison.win8@live.com> Peter Vison opeterwison.win8@live.com> Peter Vison opetervison.win8@live.com> Peter Vi	From C - optetrwison.win8@gmal.com> - - optetrwison.win8@gmal.com>
was	FILE End State File End State Final Related tensors (56 / 36) Final Related tensors (From Enal) (312 / 312) Final Related tensors FILE Final Related tensors FILE File File File File File File File File	of 7	Name 20001141_d899e914964621a.eml 20001151_d699e914964621a.eml 20001151_d699ee419684621a.eml 20001151_dc91644623544.eml 20001151_dc9164623544.eml 20001151_dc91642652072.eml 20000154_dc9164552072.eml 20000154_dc9164552072.eml 20000154_dc9164552072.eml 20000154_dc9164552072.eml 20000154_dc9164552072.eml 20000154_dc9164620072.eml 20000154_dc9164600000000000000000000000000000000000	(1) (Company Time 2on Subject Five 04/25/2013 Daily Email Five 05/10/2013 Daily Email	E Eastern Daylight Time (From local machine) To Peter Wilson cpeterwilson.win8@live.com> Peterwilson.peterwilson.win8	From CC optertwison.win8@gmai.com> optertwison.win8@gmai.com> optertwison.win8@gmai.com> optertwison.win8@gmai.com> optertwison.win8@gmai.com> com> optertwison.win8@gmai.com> Imails, the receiver
was	FITK found a total of end Retainers (36/36) Final Retaid Items (From Email) (312/312) Final Retaid Items (From Email) (312/312) Final Retaid Items (From Email) (312/312) Final Addresses Final Addresses Fi	of 7	Name Visione 20000141_d899e940ebc21a.eml 20000151_d6153ec11.eml 20000151_d6154ec12354.eml 20000151_d6154ec12354.eml 20000151_d6154ec12354.eml 20000151_d6154ec12354.eml 20000154_d6154555202.eml 20000154_d61545555202.eml 20000154_d7154555545202.eml	(****) (***********************	Comparing the sense of the	E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> E teatern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterw	From CC - optertwison.win8@gmail.com>
was	FIGURE Construction of the second sec	of 7	Name Name 2000141_d899e940e621a.emi 2000151_d919e62235eb.emi 2000151_d919e2235eb.emi 2000151_d919e2235eb.emi 2000151_d919e2364.emi 2000151_d919e2364.emi 2000151_d919e2364.emi 2000151_d919e2364.emi 2000151_d919e2364.emi 2000151_d919e2364.emi 2000151_d919e2364.emi 2000152_d9129e2364.emi 2000152_d9129e2364.emi 2000152_d9129e2364.emi 2000152_d9129e2364.emi 2000152_d9129e2364.emi 2000152_d9129e23644.emi 2000152_d9129e23644.emi 2000152_d9129e2365617.emi	(10) (10)	Comparing the sense of the	E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.wi	From CC optertwison.win8@gmal.com> opterwison.win8@gmal.com> opterwison.win8@gmal.com> opterwison.win8@gmal.com> opterwison.win8@gmal.com> opterwison.win8@gmal.com> Image: Second Secon
was	FTK found a total of the formation of th	of 7	Name Viane 20000141_0899e940e6c21a.eml 20000151_06473e615ac11.eml 20000151_0240e2235e8b.eml 20000151_0240e240235e8b.eml 20000151_0240e240235e8b.eml 20000151_0240e240235e8b.eml 20000151_0240e240236e8.eml 20000154_0240582072.eml 20000152_0272640582072.eml 20000152_027264058204 20000152_027264058204 20000152_0275556406 20000152_0275556406 20000152_0275556406 20000152_0275556406 20000152_0275556406 20000152_0275556406 20000152_0275556406 20000152_0275556406 20000152_0275556406	(b) (b) (c) (Comparing the sense of the	E Eastern Daylight Time (from local machine) To Peter Wilson opeterwilson.win8@live.com> Peterwilson opeterwilson.win	From CC optetrwison.win88gmal.com> optetrwison.win88gmal.com>
was	Final Relation of the field of	of 7	Name Name 20000141_d899e940ebc21a.eml 20000151_d910ecc2354b.eml 20000151_d910ecc2354b.eml 20000151_d910ecc2354b.eml 20000151_d910ecc2354b.eml 20000151_d910ecc2354b.eml 20000151_d910ecc2354b.eml 20000154_d910ecc2364b.eml 20000154_d910ecc2364b.eml 20000154_d910ecc2364b.eml 20000154_d910ecc2365.eml 20000152_d910ecc23654b.eml 20000152_d910ecc236565ecc1 20000152_d910ecc38566ecc1 20000152_d910ecc38566ecc1 20000152_d910ecc38566ecc1 20000152_d910ecc38566ecc1 20000152_d910ecc38566ecc1 20000152_d910ecc38566cc1 20000152_d910ecc38566cc1 20000152_d910ecc3856cc20 20000152_d910ecc3856cc20 20000152_d910ecc3856cc20 20000152_d910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910ecc3856cc20 20000152_g910eccc3856cc20 <td>(■・) (■・)</td> <td>Comparing the second seco</td> <td>E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.wi</td> <td>From C - optertwison.win8@gmail.com> </td>	(■・) (■・)	Comparing the second seco	E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peter Wilson opeterwilson.wi	From C - optertwison.win8@gmail.com>
was	FITK found a total of the set of	of 7	Name Name 20000141_d889x914964621a.eml 20000151_d889x914964621a.eml 20000151_d280x22584b.eml 20000151_d280x22584b.eml 20000151_d280x210x1 20000151_d280x210x1 20000154_d280x210x1 20000154_d280x210x1 20000154_d280x210x1 20000154_d280x210x1 20000154_d180x20x10x1 20000154_d180x20x10x10x10x10x10x10x10x10x10x10x10x10x10	(***) (***)	Comparing and Decision of	E Eastern Daylight Time (From local machine)	From CC optertwison.win88gmal.com> opterwison.win88gmal.com> opterwison.win88gmal.com> opterwison.win88gmal.com>
was	FITK found a total of the first statements (36/36) Final Related Items (From Email) (312/312) Final Addresses Final Addresses Final Related Items (From Email) (312/312) Final Items Final Related Items (From Email) (312/312) Final Items Final Related Items (From Email) (312/312) Final Related Items (From Email) (312/312)	of 7	Name Name 20000141_d899e940ebc21a.eml 20000151_d692ebc2354b.eml 20000151_d692ebc2354b.eml 20000151_d692ebc2354b.eml 20000151_d692ebc2354b.eml 20000151_d692ebc2354b.eml 20000154_d7164bc32674.eml 20000154_d7164bc32674.eml 20000154_d7164bc32702.eml 20000154_d7164bc32702.eml 20000154_d7164bc32702.eml 20000154_d7164bc32702.eml 20000154_d7164bc32702.eml 20000154_d7164bc32702.eml 20000154_d7164bc3702.eml 20000154_d7164bc370556d.eml 20000154_d7164bc370556d.eml 20000154_d7164bc37056d.eml 20000154_d7164bc37656d.eml 20000154_d7164bc37656d.eml 20000154_d7164bc37656d.eml 20000154_d7164bc37656d.eml 20000154_d7164bc37	(i) (i) (i) (i) (i) (i) (i) (i) (i)	Comparing the second seco	E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peterwilson opeterwilson.win	From CC - optertwison.win8@gmail.com>
was	Final Related tens (36/36) Final Related tens (700 Email (312/312) Final Addresses Final Addresses Final Addresses Final Related tens (36/36) Final Relat		Name Name 20000141_d899e940e621a.eml 20001512_d943e613bot1.eml 20001512_d942e2354b.eml 20001512_d942e2354b.eml 20001512_d942e24354b.eml 20001512_d942e3454.eml 20001512_d942e3454.eml 20001512_d942e3454.eml 20001514_d941f1e4552549467.eml 20001514_d951f1e4554346.eml 20001514_d951f1e4555436.eml 20001514_d9757545435368.eml 20001514_d975575454358.eml 20001514_d975575454358.eml 20001514_d975575454358.eml 20001514_d9755554358.eml 20001514_d9755554358.eml 20001514_d9755554358.eml 20001514_d9755554358.eml 20001514_d97555554358.eml 20001514_d97555554358.eml 20001514_d9755555555858.eml 20001514_d97555555555555555555555555555555555555	(■) (■)	Comparing and Department Comparing a	E Eastern Daylight Time (From local machine)	From CC - optertwison.win8@gmal.com>
was	FILE End State Final Reductions (36/36) Final Reduct Items (10/312/312) Final Reduct Items (10/312/312) Final Reduct Items (10/312/312) Final Reduct Items (10/312) Final Reduct Items (10/312) Final Reduct Items (10/312) Final Reduct Items (10/312) Final Reduct Items (10/32) Final Reduct Items (10/32	of 7	Name Name 20001141_0899e9140e6212.eml 20001151_06115e11 20001151_06125e11 20001151_06115e11 20001151_06115e11 20001151_06115e11 20001151_06115e11 20001151_06115e11 20001151_06115e11 20001151_061155e11 20001151_06115e11 20001151_06115e11 20001152_0712	(****) (****)	Compared and Control of the con	E Eastern Daylight Time (From local machine) To Peter Wilson cpeterwilson.win8@live.com> PeterWilson cpeterwilson.win	From CC optetrwison.win88gmal.com> optetrwison.win88gmal.com>
was	FIGURATION Control (36/36) Final Related Items (760 mEmail) (312/312) Final Addresses Final Addresses Final Related Items (760 mEmail) (312/312) Final Items Final Items Final Items Final Items Final Items Final Items Final Items Final Related Items (760 mEmail) (312/312) Final Items Final Items	of 7	Name Name 20000141_0809e940ebc21a.eml 20000151_0240522358b.eml 20000151_0240522358b.eml 20000151_0240522358b.eml 20000151_024058241000.eml 20000151_024058241000.eml 20000154_02564585402.eml 20000154_0256585402.eml 20000154_02565841000 20000152_0272555854000 20000152_0272555854000 20000152_0275555854000 20000152_02755558540000 20000152_0275555854000000 20000152_027555585400000000000000000000000000000000	(****) (*****) (***********	Comparing the series of t	E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peterwilson opeterwilson.win	From CC optertwison.win88gmal.com> optertwison.win88gmal
was	Final Rest Constant (36/36) Final Rest Rest Constant (37/36) Final Rest Rest Constant (37/36) Final Rest Const Constant (37/36) Final Rest Constant (37/36)	of 7	Name Name 20000141_0809e914904621a.eml 2000151_0611_eml 20000151_0611_eml 2000151_0611_eml 2000151_0611_eml <td>(****) (****)</td> <td>Comparing and Department of the second de</td> <td></td> <td>From CC -potertwison.win8@gmal.com> </td>	(****) (****)	Comparing and Department of the second de		From CC -potertwison.win8@gmal.com>
was	FTK found a total (Enal Relations) (36/36) Frail Related Items (Yon Enal) (312/312) Frail Related Items (Yon Enal) (312/312) Frail Relatives Frail Relati	of 7	Name Name 20000141_0899e940e6c21a.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000151_0240e2c235eb.eml 20000152_0272eml 20000152_072eml 20000152_072655ebe2c2 20000152_072655ebe2c2 20000152_072655ebe2c2 20000162_07275555ebe2c2 20000162_07275555564c2 20000161_0507677767555564c2 </td <td></td> <td>Constant Section 2014 Constant Section 2014 Section</td> <td>E Eastern Daylight Time (from local machine)</td> <td>From CC optetrwison.win88gunal.com> optetrwison.win88gunal.com> optetrwison.win88gunal.com> optetrwison.win88gunal.com></td>		Constant Section 2014 Constant Section 2014 Section	E Eastern Daylight Time (from local machine)	From CC optetrwison.win88gunal.com> optetrwison.win88gunal.com>
was	FIGURE Constraints (36/36) Final Related Items (760 mEmail) (312/312) Final Addresses Final Addresses Final Related Items (760 mEmail) (312/312) Final Items (97/87) Final Items (97/87) Final Items (97/87) Final Items (97/87)	of 7	Name Name 20000141_0809e940ebc21a.eml 20000151_0240es2354b.eml 20000151_0240es2354b.eml 20000151_0240es2354b.eml 20000151_0240es2354b.eml 20000151_0240es2000.eml 8 Filtered: 8 Filtered: 8 R amail: colspan="2">colspan="2">Colspan="2" Colspan="2"	(e) (e) (e) (e) (e) (e) (e) (e) (e)	Construction Constender Constender Construction Construction Const	E Eastern Daylight Time (From local machine) To Peter Wilson opeterwilson.win8@live.com> Peterwilson opeterwilson.wi	From C opetertwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com> opeterwison.win8@gmal.com>
was	FILE End State File End State Final Reduced Items (\$6/36) Final Reduced Items (From Enal) (312/312) Final Reduced Items (From Enal) (312/312) Final Reduced Items (From Enal) (312/312) File Enal Addresses File Enal Addresses File Enal Reduce Item (From Enal) (312/312) File Enal Reduce Items (From Enal) (312/312) File Enal Reduce Item	of 7 (@ gr) arch index) arch	Name Name 20000141_0809e914086212.eml 20000150_2000222358b.eml 20000150_2000222358b.eml 2000111_0756952491682.eml 20000111_0756952491682.eml 20000114_0756952491682.eml 2000014_0756952491682.eml 2000014_0756952491682.eml 2000014_0756952491682.eml 2000014_0756952491682.eml 2000014_0756952491682.eml 2000014_07569554916 2000014_1596971bd68916 2000014_1596971bd689164		Constant Section Constant Cons	E Eastern Daylight Time (From local machine) E Castern Daylight Time (From local machine) E Castern Daylight Time (From local machine) E Castern Daylight Time (From local machine) E Castern Day	Image: Constraint of the second se
was	FTK found a total (Enal Related Items (760 161) Final Related Items (700 Enal) (312/312) Final Related Items (700 Enal) (312/312) Final Related Items (700 Enal) (312/312) Final Addresses Final Addresses Final Related Items (700 Enal) (312/312) Final Related Items (700 Enal	of 7	Name Name 20000141_0899e940e8c21a.eml 20000151_0240e8c2354b.eml 20000151_0240e8c2354b.eml 20000151_0240e8c2354b.eml 20000151_0240e8c2354b.eml 20000151_0240e8c2354b.eml 20000151_0240e8c2354b.eml 20000154_025002.eml 20000154_025002.eml 20000154_025002.eml 20000154_025002.eml 20000152_072555002.eml 20000152_0725555002.eml 20000154_075555002.eml 20000154_075555002.eml 20000154_075555002.eml 20000154_075555002.eml 20000154_075555002.eml 20000154_075555002.eml	Sumt Time H22(20) 310- H22(20) 312- St/220) 312- St/220) 312- St/220) 312- St/220) 372- Total: 8 Total: 8 Total: 8 Vere re peterw vere re peterw vere re submit Time 4/26(20) 312- St/220) 372- 4/25(20) 312- St/220) 372- St/220	Comparison of the second	E Eastern Daylight Time (From local machine)	From CC optetrwison.win8@gmail.com> optetrwison.win8@gmail.com> optetrwison.win8@gmail.com> optetrwison.win8@
was	Final Rest States Final Rest Recting (58/36) Final Rest Recting (58/36) Final Rest Recting (77) Final Rest Recting (7	of 7 '@gi archine' arch	Name Name 20000141_0809e914926212.eml 2000151_021672825825.eml 2000151_021672825825.eml 2000151_02167282582582.eml 2000151_02167282582582.eml 2000151_02167282582582.eml 2000151_02167282582582.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_0216728258202.eml 2000151_021672845826828.eml 2000151_0216728458282882867817.eml 20000151_021679459458398.eml 20000151_0216794583982867817.eml 20000151_021694594583982867817.eml 20000151_02169459458398.eml 20000151_02169459458398.eml 20000151_02169459458398.eml 20000151_02169459458398.eml 20000151_021692651828389.eml 20000151_021692651828389.eml 20000151_021692653892.eml 20000151_021692653892.eml 20000151_021692653892.eml		Consider in the second se	E Eastern Daylight Time (From local machine)	From C -petertwison.win8@gmal.com>
was	FTK found a total of either peterwilson.win7 Figure Convey End Redections (36/36) Figure Redections (10/2) Figure Redection (of 7 '@gj loaded loaded loaded	Name Name 20001141_0899e9140e6212.a.eml 20001151_06115-000115-00115-00115-000115-00115-0011		Comparison of the second	E Eastern Daylight Time (from local machine)	From CC optetrwison.win88gmal.com> optetrwison.win88gmal.com>

Cilial Status			• • • Email	Display Time Zone: Eastern Daylight Time (From local machine)		
	ents (36 / 36) Items (From Email) (312 / 312)	Name rit black no bar.jpg	Submit Time Subject	To	From	
	(7) al(8/8)	rit_white_no_bar.jpg				
Email Archives		rit_white_no_bar.jpg				
Email Addresses	H	 04242013attachment.txt.txt tiger_walking_rit.jpg 				
- 🔤 Email (67) 67)		 tiger_walking_rit_color.jpg 05012013attachment.txt 				
	la	2 05032013attachment.txt				
		tiger_walking_rit_color.jpg				
	Loa	aded: 36 Filtered: 36	Total: 36 Highlighted: 1	Checked: 0 Total LSize: 0 B		-
			Figure 85 Email	Attachments		
tunatelv	when I view ar	n email that v	vould have had an	attachment sent with it I see info	rmation per	taini
· · · 1· · · · · ·	h	4			r	
tachmen	, but am unable	to view the a	attachments thems	serves:		
Content Viev	er [2000015c_960a015d5a	85c8.eml]				
Hex Text Filt	red Natural					
ss 🗗						
05/0	01/2013	Daily E	mail with	Text and Picture		<u> </u>
05/0 Atta)1/2013 chments	Daily E	mail with	Text and Picture		*
05/0 Atta	01/2013 chments	Daily E	mail with	Text and Picture		*
05/0 Atta ^{From:}	01/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@< td=""><td>Daily E Wilson.Win7@live.c tterWilson.Win7@gr Jive.com></td><td>com> mail.com>, Windows8 Gmai</td><td>Text and Picture</td><td></td><td>*</td></peterwilson.win8@<></pe </peter 	Daily E Wilson.Win7@live.c tterWilson.Win7@gr Jive.com>	com> mail.com>, Windows8 Gmai	Text and Picture		*
05/0 Atta From: To: Subject:	01/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em</peterwilson.win8@ </pe </peter 	Daily E Wilson.Win7@live.c terWilson.Win7@gr live.com> wil with Text and P	com> mail.com>, Windows8 Gmai	Text and Picture		*
05/0 Atta	01/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15</peterwilson.win8@ </pe </peter 	Daily E Wilson.Win7@live.c terWilson.Win7@gr live.com> nail with Text and P 5:31:29 +0000	com> mail.com>, Windows8 Gmai	Text and Picture		*
O5/O Atta	01/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.c</peterwilson.win8@ </pe </peter 	Daily E Wilson.Win7@live.c terWilson.Win7@gr live.com> mail with Text and P 5:31:29 +0000 om	com> mail.com>, Windows8 Gmai	Text and Picture		*
Contemporation of the second s	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.ct art, Type: image/jpeg; r</peterwilson.win8@ </pe </peter 	Daily E Wilson.Win7@live.c. terWilson.Win7@gr live.com> aail with Text and P 5:31:29 +0000 om name="tiger_walking	mail with	Text and Picture	1	*
Contemporation of the second s	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily En Wed, 1 May 2013 15 eterWilson.Win7@live.ct art, Type: image/jpeg; r art, Type: image/jpeg; r</peterwilson.win8@ </pe </peter 	Daily E Wilson.Win7@live.c terWilson.Win7@gr live.com> ail with Text and P 5:31:29 +0000 om name="tiger_walking name="tiger_walking	mail with com> mail.com>, Windows8 Gmai Picture Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta	Text and Picture] : 0 bytes]	
Control Contro	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.c urt, Type: image/jpeg; r urt, Type: image/jpeg; r urt, Type: text/plain; na</peterwilson.win8@ </pe </peter 	Daily E	mail with com> mail.com>, Windows8 Gmai Picture Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta	Text and Picture] : 0 bytes] Size: 0 bytes]	
Contraction of the second seco	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.co Int, Type: image/jpeg; r Int, Type: image/jpeg; r Int, Type: image/jpeg; r Int, Type: text/plain; na</peterwilson.win8@ </pe </peter 	Daily E Wilson.Win7@live.c. terWilson.Win7@gr live.com> aall with Text and P 5:31:29 +0000 om name="tiger_walking name="tiger_walking name="tiger_walking	mail with mail.com> windows8 Gmai Picture Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta	Text and Picture] : 0 bytes] Size: 0 bytes]	
Control Contro	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.cc art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: text/plain; na</peterwilson.win8@ </pe </peter 	Daily E	mail with mail.com> windows8 Gmai Picture Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta	Text and Picture] : 0 bytes] Size: 0 bytes]	*
Content-T	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.ci art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: text/plain; na sion: 1.0 e: Normal ype: multipart/mixed; b</peterwilson.win8@ </pe </peter 	Daily E	mail with com> mail.com>, Windows8 Gmai Victure Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta B6-0F5C-47AC-879D-A029	Text and Picture] : 0 bytes] Size: 0 bytes]	*
Content-T Attachmen	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.cr art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: text/plain; na cion: 1.0 e: Normal pe: multipart/mixed; b at-0: tiger_walking_rit.jj</peterwilson.win8@ </pe </peter 	Daily E	Email with com> mail.com>, Windows8 Gmai Victure Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta B6-0F5C-47AC-879D-A029	Text and Picture] : 0 bytes] Size: 0 bytes]	*
Content-T Attachmen	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.cr art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: text/plain; na cion: 1.0 e: Normal rpe: multipart/mixed; b at-0: tiger_walking_rit.j at-1: tiger_walking_rit.c</peterwilson.win8@ </pe </peter 	Daily E	Email with com> mail.com>, Windows8 Gmai Victure Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta B6-0F5C-47AC-879D-A029	Text and Picture] : 0 bytes] Size: 0 bytes]	*
Content-T Attachmen	D1/2013 chments Live Account <peter Windows7 Gmail <pe <peterwilson.win8@ 05/01/2013 Daily Em Wed, 1 May 2013 15 eterWilson.Win7@live.ci art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: image/jpeg; r art, Type: text/plain; na cion: 1.0 e: Normal art of tiger_walking_rit_ci at-0: tiger_walking_rit_ci at-2: 05012013attachm</peterwilson.win8@ </pe </peter 	Daily E	mail with com> mail.com>, Windows8 Gmai Picture Attachments g_rit.jpg", Disp: attachmen g_rit_color.jpg", Disp: atta achment.txt.txt", Disp: atta	Text and Picture] : 0 bytes] Size: 0 bytes]	*

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 Registry 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	Туре	Data
80 MRUListEx	REG_BINARY	13 00 00 00 12 00 00 01 10 00 00 10 00 00 00 00 00 00
80 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
80 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
80 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
80 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
80 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
80 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
80 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
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 .
88 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 .
80 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 .
80 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 .
807	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
806	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
88 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
86 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
883	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
88 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
R o	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

Figure 87 OpenSavePIDIMRU 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	lF	50	ΕO	4F	DO	20-EA	ЗA	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	СО	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	·1·3·2·. ·d·1·1·,
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·l····Bî···W
0Ъ0	69	6E	64	6F	77	73	38	00-00	ЗE	00	08	00	04	00	EF	indows8··>····ï
0c0	ΒE	68	42	CD	26	98	42	EE-OB	2 A	00	00	00	DЗ	32	01	‰hBÍ&·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
OfO	00	38	00	00	00	18	00	80-00	31	00	00	00	00	00	8E	·8·····1····
100	42	66	41	11	00	44	4F	43-55	$4 \mathbb{D}$	45	7E	31	00	00	68	BfA · · DOCUME~1 · · h
110	00	08	00	04	00	EF	ΒE	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	ЗE	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	·1·1·, ·- ·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	ΒE	00	ly.txt·P····i¾·
1a0	00	00	00	00	00	00	00	2 A- 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:

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

Table 14 OpenSavePIDIMRU Applications

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

 $Version \\ Explorer \\ ComDlg32 \\ Last \\ Visited \\ MRU we are able to see a listing of applications that were recently used to be a listing of application \\ MRU we are able to see a listing of applications that were recently used to be a listing of application \\ MRU we are able to see a listing of applications that were recently used to be a listing of application \\ MRU we are able to see a listing of applications that were recently used to be a listing of applications \\ MRU we are able to see a listing of applications \\ MRU we are able to see a listing \\ MRU we are able to see a listing \\ MRU we are able to see a listing \\ MRU we are able to see a listing \\ MRU we are able to see a listing \\ MRU we are able \\ MRU we are a$

open or save the files listed in the OpenSavePIDIMRU registry key:

	Name	Туре		0)ata												
		REG_BI	NARY	0	0 00 0	0 00 02	2 00 00	00 01 (00 00 00 FF Ff	FF FF							
	80 0	REG_BI	NARY	6	E 00 6	F 00 74	00 65	00 70 (00 61 00 64 00	0 2E 00	65 00	78 00 6	55 00 0	0 00 1	ŧ 00 1F	50 E0	4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 19
	1002 2001	REG_BI		÷ د	9 UU 6 6 00 6	5 UU 78 9 00 72	00 45	00.6CT	UU 6F UU 72 U 00 4E 00 79 0(0 65 UU 3 25 OC) 2E UU	65 UU - 79 00 4	/8006	0.00.1/	JUU 14 1 00 15	00 1F	44 47 1A U3 59 72 3F A7 44 89 C5 55 95 FE 6B 30
	ing i	KLG_DI	INMENT	, i	0 00 0	9 00 72	. 00 05	00 00 1		J 2L UU	05 00	/0 00 (5000	0 00 1	100 11	11 17	IN 03 39 72 31 A7 44 09 C3 33 931 E 05 30 EE 20 0
	Figure 89 LastVisitedPidMRU Registry Key																
As v	As was the case with the previous registry key, the data portion appears in hexadecimal but Registry Viewer can																
conv	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	EO	4F	DO	20	e·x·e····PàOĐ
	020	EA	3A	69	10	A2	D8	08	00-2B	30	30	9D	19	00	2F	43	ê:i.eØ+00/C
	030	34	50	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·l···hBÍ
	0.50	26	11	00	55	73	65	72	73-00	60	00	08	00	04	00	EF	& ···Users · ` · · · · · ï
	060	BE	FA	40	СО	20	68	42	CD-26	2A	00	00	00	28	00	00	%ώβÅ.hBÍ«*···(··
	070	00	00	00	01	00	00	00	00-00	00	00	00	00	36	00	00	
	080	00	00	00	55	00	73	00	65-00	72	00	73	00	00	00	40	···II·s·e·r·s··0
	090	00	73	00	68	00	65	00	60-00	60	00	33	00	32	00	2E	-s-h-e-1-1-3-2
	0a0	00	64	00	60	00	60	00	20-00	2D	00	32	00	31	00	38	·d·1·1·.·-·2·1·8
	010	00	31	00	33	00	00	00	14-00	56	00	31	00	00	00	00	-1-3V-1
	0c0	00	98	42	EE	0B	10	00	57-69	6E	64	6F	77	73	38	00	··Bî···Windows8·
	0b0	00	ЗE	00	08	00	04	00	EF-BE	68	42	CD	26	98	42	EE	·>····ï¾hBÍ&·Bî
	0e0	OB	2A	00	00	00	D3	32	01-00	00	00	07	00	00	00	00	·*···Ó2·····
	0£0	00	00	00	00	00	00	00	00-00	00	00	57	00	69	00	6E	
	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	$UME \sim 1 \cdot h \cdot \cdots \cdot 3 \lambda h$
	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	ЗE	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	60	00	60	·s···@·s·h·e·1·1
	170	00	33	00	32	00	2E	00	64-00	6C	00	60	00	20	00	2D	·3·2·. ·d·1·1·. ·-
	180	00	32	00	31	00	37	00	37-00	30	00	00	00	18	00	00	.2.1.7.7.0
	190	00															
	200	1															1
			Fig	gure	90	HE	X aı	nd A	SCII D	ata	RE	G_F	BIN	ARY	7 O I	Last	tVisitedMRU
17	05012013Daily.lnk																
----	--																
16	httpwww.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	httpwww.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	httpmail.live.comlnk																

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:

Name	Туре	Data
😅 DaylightBias	REG_DWORD	0xFFFFFFC4 (4294967236)
alightName 🛃	REG_SZ	@tzres.dll,-111
🔀 StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00 00
😅 StandardBias	REG_DWORD	0×00000000 (0)
and ard Name	REG_SZ	@tzres.dll,-112
Bias	REG_DWORD	0x0000012C (300)
📴 DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
M TimeZoneKeyName	REG_SZ	Eastern Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0×00000000 (0)
activeTimeBias	REG_DWORD	0x000000F0 (240)

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	Туре	Data
an ProfileGuid	REG_SZ	{02C9AC7A-5F87-46A4-BCFE-4D7C0275FCAC}
Description	REG_SZ	Network 2
🔣 Source	REG_DWORD	0×00000008 (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	Туре	Data
and ProfileGuid	REG_SZ	{963DD6CD-43F6-4369-A76F-950D75D07E4D}
Description	REG_SZ	Network
🔀 Source	REG_DWORD	0×00000008 (8)
a)DnsSuffix	REG_SZ	localdomain
a 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:

Last Written Time4/21/2013 20:04:35 UTCSID unique identifier1001User NameWindows8Full NamePeter WilsonLogon Count9Last Logon Time4/21/2013 20:04:31 UTCLast Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue	-	Key Properties		
SID unique identifier1001User NameWindows8Full NamePeter WilsonLogon Count9Last Logon Time4/21/2013 20:04:31 UTCLast Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Last Written Time	4/21/2013 20:04:35 UTC	
User NameWindows8Full NamePeter WilsonLogon Count9Last Logon Time4/21/2013 20:04:31 UTCLast Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		SID unique identifier	1001	
Full NamePeter WilsonLogon Count9Last Logon Time4/21/2013 20:04:31 UTCLast Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		User Name	Windows8	
Logon Count9Last Logon Time4/21/2013 20:04:31 UTCLast Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Full Name	Peter Wilson	
Last Logon Time4/21/2013 20:04:31 UTCLast Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Logon Count	9	
Last Password Change Time4/21/2013 20:04:35 UTCExpiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedfalseHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Last Logon Time	4/21/2013 20:04:31 UTC	
Expiration TimeNeverInvalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Last Password Change Time	4/21/2013 20:04:35 UTC	
Invalid Logon Count0Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Expiration Time	Never	
Last Failed Login TimeNeverAccount DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Invalid Logon Count	0	
Account DisabledfalsePassword RequiredfalseCountry Code1 (United States)Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Last Failed Login Time	Never	
Password RequiredfalseCountry Code1 (United States)Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Account Disabled	false	
Country Code1 (United States)Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Password Required	false	
Hours AllowedAnytimeHas LAN Manager PasswordfalseHas NTLMv2 Passwordtrue		Country Code	1 (United States)	
Has LAN Manager Password false Has NTLMv2 Password true		Hours Allowed	Anytime	
Has NTLMv2 Password true		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

- 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-towindows-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-removedconsumer-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-userexperience.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-cloudpowered-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-browsingin-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-towindows-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-andwindows-phone-windows-live-reimagined.aspx. [Accessed 4 April 2013].
- 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-filehistory.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].