Oleg Skulkin, Scar de Courcier

Windows Forensics Cookbook

61 recipes to help you analyze Windows systems

Packt

Windows Forensics Cookbook

61 recipes to help you analyze Windows systems

Oleg Skulkin
Scar de Courcier

Packt

BIRMINGHAM - MUMBAI

Windows Forensics Cookbook

Copyright © 2017 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: August 2017

Production reference: 1030817

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78439-049-5

www.packtpub.com

Credits

Authors
Oleg Skulkin
Scar de Courcier

Reviewer
Igor Mikhaylov

Acquisition Editor
Meeta Rajani

Content Development Editor
Devika Battike

Technical Editor
Manish Shanbhag

Production Coordinator
Aparna Bhagat

Copy Editor
Juliana Nair

Project Coordinator
Judie Jose

Proofreader
Safis Editing

Indexer
Aishwarya Gangawane

Graphics
Kirk D'Penha

About the Authors

Oleg Skulkin is a digital forensic enthusional (enthusiast and professional) from Sochi, Russia. Having more than 5 years of experience, he solves lots of different cases involving digital evidence for the Ministry of Internal Affairs of Russia. Also, you can find his articles both in Russian and foreign magazines. Finally, Oleg is a very active blogger, and he updates Cyber Forensicator's blog daily.

> *I would like to thank my mom and wife for all the support, Scar, Igor, the Packt team, and all my real and online digital forensic friends, who inspire me to keep going.*

Scar de Courcier is Senior Editor at digital forensics website Forensic Focus. She also works as an independent consultant on online and offline child protection projects. In her spare time, she enjoys swimming, pretending she lives on the USS Voyager, and hanging out with her cat.

> *Firstly, I must thank Jamie Morris for his guidance, help and most of all patience over the past few years. My co-author Oleg for having my back, and the team at Packt for their help and understanding. All my online and offline DFIR buddies, for their suggestions and support; special thanks to Christa Miller, Daryl Pfeif and Mattia Epifani, for taking my place at conferences and making this whole process easier. And finally, a shout-out to Ali Gray, for her encouragement in the final chapter.*

About the Reviewer

Igor Mikhaylov has been working as a forensic examiner for 20 years. During this time, he has visited a lot of seminars and training classes by top digital forensic companies (such as Guidance Software, AccessData, and Cellebrite) and forensic departments of government organizations of the Russian Federation. He has experience and skills in computer forensics, incident response, cell phone forensics, chip-off forensics, malware forensics, data recovery, digital images analysis, video forensics, and big data, etc.

He has written three tutorials on cell phone forensics and incident response for Russian forensic examiners.

www.PacktPub.com

For support files and downloads related to your book, please visit `www.PacktPub.com`.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

Mapt

`https://www.packtpub.com/mapt`

Get the most in-demand software skills with Mapt. Mapt gives you full access to all Packt books and video courses, as well as industry-leading tools to help you plan your personal development and advance your career.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print, and bookmark content
- On demand and accessible via a web browser

Customer Feedback

Thanks for purchasing this Packt book. At Packt, quality is at the heart of our editorial process. To help us improve, please leave us an honest review on this book's Amazon page at `https://www.amazon.com/dp/1784390496/`.

If you'd like to join our team of regular reviewers, you can e-mail us at `customerreviews@packtpub.com`. We award our regular reviewers with free eBooks and videos in exchange for their valuable feedback. Help us be relentless in improving our products!

Table of Contents

Preface

Windows Forensics Cookbook covers recipes to overcome challenges and carry out effective investigations easily on a Windows platform. You will begin with a refresher of *Digital Forensics and Evidence Acquisition*, which will help you to understand the challenges faced while acquiring evidence from Windows systems. Next, you will learn how to acquire Windows memory and analyze Windows systems with modern forensic tools. The book will also cover more in-depth elements of forensic analysis, such as how to analyze data from Windows system artifacts, parsing data from the most commonly-used web browsers and email clients, and effective reporting in digital forensic investigations.

You will learn how Windows 10 is different from previous versions and how you can overcome the specific challenges it brings. Finally, you will learn how to troubleshoot issues that arise while performing digital forensic investigations.

By the end of the book, you will be able to carry out forensic investigations efficiently.

What this book covers

`Chapter 1`, *Digital Forensics and Evidence Acquisition*, will give you a brief overview of digital forensics as a science, and will cover the basics of digital evidence acquisition, examination and reporting.

`Chapter 2`, *Windows Memory Acquisition and Analysis*, will guide you through Windows memory acquisition with Belkasoft RAM Capturer and DumpIt. After you will learn how to analyze memory images with Belkasoft Evidence Center and Volatility.

`Chapter3`, *Windows Drive Acquisition*, will guide you through the acquisition of the main source of Windows forensic artifacts – hard and solid state drives. You will learn how to create forensic images with FTK Imager and DC3DD, and also how to mount them with Arsenal Image Mounter.

`Chapter4`, *Windows File Systems Analysis*, will guide you through the analysis of the most common Windows filesystem, New Technology File System or NTFS, with the Sleuth Kit. Also, you will learn how to recover deleted files from both NTFS and its descendant, ReFS, using Autopsy, ReclaiMe Pro, and PhotoRec.

`Chapter5`, *Windows Shadow Copies Analysis*, will show you how to browse and copy files from VSCs with ShadowCopyView. Also you will learn how to mount these copies with VSSADMIN and MKLINK, and analyze their data with Magnet AXIOM.

`Chapter6`, *Windows Registry Analysis*, will show you how to extract data from the Windows Registry with Magnet AXIOM and the RegRipper. Also, you will learn how to recover deleted Registry artifacts with the Registry Explorer.

`Chapter 7`, *Main Windows Operating System Artifacts*, will introduce you to the main Windows forensic artifacts, including the Recycle Bin items, Windows Event Logs, LNK files, and Prefetch files. You will learn how to analyze these artifacts with EnCase Forensic, Rifiuti2, Magnet AXIOM, FullEventLogView, EVTXtract, LECmd, Link Parser, PECmd, and Windows Prefetch Carver.

`Chapter 8`, *Web Browser Forensics*, will guide you through the analysis of the most popular Windows web browser with BlackBagBlackLight, Magnet Axiom, and Belkasoft Evidence Center. Also, you will learn how to extract browser data from a paging file.

`Chapter 9`, *Email and Instant Messaging Forensics*, will show you how to analyze artifacts of the most popular Windows email clients – Microsoft Outlook and Mozilla Thunderbird, and the instant messaging application Skype. Also, you will learn how to extract webmail artifacts from a forensic image.

`Chapter 10`, *Windows 10 Forensics*, will introduce you to Windows 10—specific artifacts, such as Cortana, the Mail app, Xbox app, and notifications. You will learn where the data is stored, its format, and how to extract and analyze it.

`Chapter 11`, *Data Visualization*, will show you how to make your forensic reports even better with data visualization techniques. You will learn how to use these techniques in Forensic Toolkit (FTK), Autopsy, and Nuix.

`Chapter 12`, *Troubleshooting in Windows Forensic Analysis*, will teach you how to solve problems with your forensic software, both commercial and free/open source; show you what to do if processes fail, why it's important to analyze false positives, give you recommendations on your first steps in digital forensics; and provide a nice list of sources for further reading.

What you need for this book

The following software is required for this book:

- Arsenal Image Mounter
- Autopsy
- Belkasoft Evidence Center
- Belkasoft RAM Capturer

- BlackBagBlackLight
- dc3dd
- DumpIt
- EnCase Forensic
- EVTXtract
- FTK
- FTK Imager
- FullEventLogView
- Intella
- LECmd
- Link Parser
- Magnet AXIOM
- Nuix
- PECmd
- PhotoRec
- ReclaiMe Pro
- Registry Explorer
- RegRipper
- Rifiuti2
- ShadowCopyView
- SkypeLogView
- The Sleuth Kit
- Volatility
- Windows Prefetch Carver

Most of the commercial tools from this list have trial versions available for downloading for free. Download links are provided in the chapters.

Who this book is for

If you are a forensic analyst and incident response professional who wants to solve computer forensics investigations for the Windows platform, then this books is for you.

Sections

In this book, you will find several headings that appear frequently (Getting ready, How to do it, How it works, There's more, and See also).

To give clear instructions on how to complete a recipe, we use these sections as follows:

Getting ready

This section tells you what to expect in the recipe, and describes how to set up any software or any preliminary settings required for the recipe.

How to do it…

This section contains the steps required to follow the recipe.

How it works…

This section usually consists of a detailed explanation of what happened in the previous section.

There's more…

This section consists of additional information about the recipe in order to make the reader more knowledgeable about the recipe.

See also

This section provides helpful links to other useful information for the recipe.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, path names, dummy URLs, user input, and Twitter handles are shown as follows: "So in our case, it's `D:\Belkasoft Memory Forensics Test`."

Any command-line input or output is written as follows:

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 malfind -p 868 --dump-dir
X:Stuxnet
```

New terms and important words are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "The first pane displays information about detected shadow copies, including name, **Explorer path**, **Volume path**, **Created Time**, and so on."

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Downloading the color images of this book

We also provide you with a PDF file that has color images of the screenshots/diagrams used in this book. The color images will help you better understand the changes in the output. You can download this file from `https://www.packtpub.com/sites/default/files/downloads/WindowsForensicsCookbook_ColorImages.pdf`.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books-maybe a mistake in the text or the code-we would be grateful if you could report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **Errata Submission Form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website or added to any list of existing errata under the Errata section of that title.

To view the previously submitted errata, go to `https://www.packtpub.com/books/content/support`and enter the name of the book in the search field. The required information will appear under the **Errata** section.

Piracy

Piracy of copyrighted material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works in any form on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors and our ability to bring you valuable content.

Questions

If you have a problem with any aspect of this book, you can contact us at `questions@packtpub.com`, and we will do our best to address the problem.

1

Digital Forensics and Evidence Acquisition

In this chapter, well cover the following recipes:

- Identifying evidence sources
- Acquiring digital evidence
- Ensuring evidence is forensically sound
- Writing reports
- Digital forensic investigation: an international field
- Challenges of acquiring digital evidence from Windows systems

Introduction

Digital forensics is an expansive term that can cover a multitude of subject areas. Broadly speaking, it refers to the investigation of crimes committed on, or with the use of, a computing device. Several years ago, this may have only been applicable to cases in which an investigator was looking at financial fraud, intellectual property theft, or similar cases where computers are, by definition, necessary in order to commit the crime.

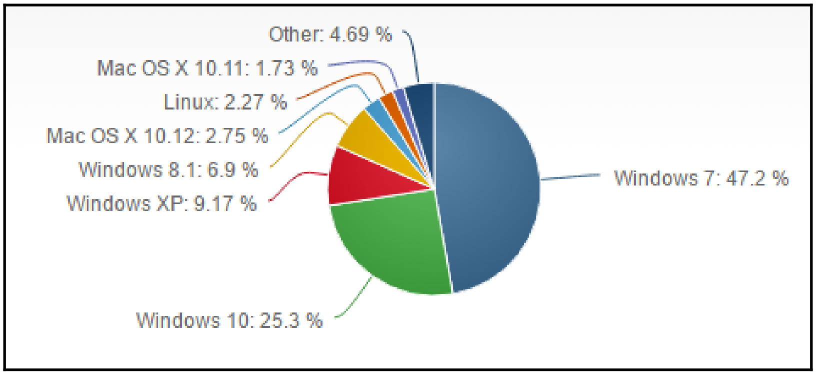
In today's world however, the proliferation of digital devices is such that even a crime that seems to be unrelated to computing—a house burglary where jewellery is stolen, for example, or the abduction of a child walking home from school—can involve a whole host of digital evidence.

Digital evidence refers to anything relevant to an investigation that can be found on a digital device. Increasingly, digital devices can refer to almost anything around us - not only computers and phones, but also cars, televisions, refrigerators, and heating systems.

Digital forensics as a discipline does not deal solely with solving crimes. HR matters in companies, private or civil cases, as well as day-to-day data recovery, can all fall under the digital forensics bracket. It is reasonable to state, therefore, that not only is digital forensics a huge field, it is also expanding. For this reason, in this book, we have decided to focus on one particular aspect of digital forensics: the forensic analysis of Windows operating systems.

Why Windows?

We could have chosen any number of operating systems as the subject of this book, not to mention the myriad smartphones and other connected devices that crop up in digital forensic investigations. Windows is, however, a popular choice of operating system for the average computer user, and for businesses — recent figures from **NetMarketShare** indicate that Windows takes up over 88% of the market. The following diagram demonstrates the market share of Windows as opposed to Mac, Linux, and other operating systems.



Regardless of whether you're working in law enforcement, in a digital forensics corporation, as an academic researcher in the field, or for yourself as a freelance investigator, the chances are that at some point you will come up against Windows systems.

Our goal in writing this book is to create a kind of *cookbook*, allowing you to dip in and out and use the recipes to aid in your investigations.

The range of available operating systems and programs that are frequently run on Windows machines makes it difficult to provide a full guide. This is particularly when we take into consideration the recent overhaul resulting in Windows 8, Windows 8.1, and Windows 10, which refer to programs as applications and look somewhat different from earlier versions both forensically and from a user experience point of view. To the best of our ability, we have tried throughout this book to highlight the most salient points in investigation and to discuss the broad implications of the changes in more recent versions.

Windows file system

Windows machines use NTFS, which used to stand for New Technology filesystem, although the acronym has now become obsolete. All versions of Windows run on NTFS as default.

The main thing to remember about NTFS is that everything is a file. The idea behind the filesystems creation was that it would be easily scalable, as well as being secure and reliable at all levels. This does present some unique challenges for forensic investigation and administrative usage, however knowing that any file can be located anywhere on the system makes it challenging to understand precisely what one is looking at when analyzing a machine.

The **Master File Table** (**MFT**) is the basis of the filesystem. In here, we find all the relevant information concerning files. It is worth noting that the first entry in the MFT is an entry that refers to the MFT itself, which can confuse people who are new to Windows filesystem analysis.

One of the most important elements in Windows investigations is the registry, where keys containing information regarding the configuration of the system, along with other forensic gems are stored. Tools such as RegEdit and RegRipper can be very useful in registry analysis, as can many of the more widely used general forensic programs, such as **EnCase** and **BlackLight**.

We will discuss the specifics of various investigative elements within the Windows NT filesystem throughout the book. For the moment, the most pertinent points to remember are that everything in NTFS is a file; that the master file table forms the base of the filesystem; and that the registry contains useful system configuration information.

Identifying evidence sources

As any digital forensic investigator will know, one of the main challenges posed by almost any case is the sheer amount of data and number of sources available to be worked through. A useful skill to have is the ability to look through the sources of evidence involved with a case and make a value judgement as to which will probably be the most useful.

From the beginning of the case, this can take the form of ascertaining which physical items to remove from a crime scene—computers and mobile phones are almost always seized, but what about USB sticks, smart televisions, and satellite navigation systems? How do you even get a WiFi connected refrigerator into a Faraday bag?

Jokes aside, once an investigator has identified the items from which they are going to attempt to extract evidence, the next hurdle is to work out which bits of evidence will be the most relevant, and where those can be found.

In Windows systems, there are several elements that will prove to be useful across many different types of investigations. While some will vary from case to case—looking for evidence of intellectual property theft or financial fraud will differ hugely from the sources you'd be locating in a child protection investigation, for instance on the whole, the following sources of evidence can generally provide useful information from which you can then extrapolate further.

In older Windows versions (around the time of XP and 2000), there were fewer programs to deal with, and therefore fewer sources of potential evidence, but there was also less room for confusion. XP was when Windows began to support the NT filesystem, which gave a boost to the previous FAT setup and allowed for more in—depth analysis of the system.

Prefetch files were introduced in XP, and swiftly became one of the most pertinent sources of evidence, which is still the case today. The aim from a user experience perspective was essentially to speed things up. Prefetch files take note of which programs are used most frequently and make sure that those programs are pre-loaded into the memory, so that when a user boots up a machine and then tries to access one of the programs, it will load more quickly. From a forensic point of view, this means that prefetch files provide a wealth of information regarding a user's general computer habits—which programs they use most often, and to some extent, how they are being used. Prefetch files are stored in the `%SystemRoot%Prefetch` directory and will be discussed in more depth in `Chapter 7`, *Main Windows System Artifacts.*

Subsequent Windows updates introduced increasingly complex elements, one of the most pertinent of which is **BitLocker**.

BitLocker provides full volume encryption and also includes a version for portable devices, called **BitLocker To Go**. Provided that the password is known, decryption of BitLocker information is relatively straightforward and can be performed using a range of forensic software, some of which will be detailed later in this book. The simplest way to ascertain whether a volume has been encrypted using BitLocker is to look for `-FVE-FS-` in the volume header. Once this has been determined and the password has been found or recovered, tools such as FTK or EnCase can be used to decrypt the information.

Around the same time BitLocker was introduced, with the release of Windows Vista, the way in which user accounts are structured within Windows also changed. This is mainly noticeable from the perspective of the user themselves, in that the main change is that many system-wide modifications that could previously be made by any user can now only be made by an administrator. This can also be an important point forensically, particularly in cases where a computer has multiple users, only one of whom has access to the administrative password.

Internet Explorer and its successor, Microsoft Edge, have been overhauled repeatedly throughout the years. We will take a much closer look at Edge later on in this book, however, for the moment, it is possible to say that there is a wealth of information to be found within internet browsers. Arguably one of the most important elements within Internet Explorer is the cache, which contains information regarding the pages a user has visited and any content that has been downloaded.

Private browsing is one of the most commonly misconceived options by the end users of Windows systems: while this may prevent other people in the household from uncovering a users secret internet habits, it is of course still open to forensic investigation.

Increasingly, we are seeing users becoming more aware of the level of information that can be gleaned using digital forensic methods, and in recent years, privacy options within operating systems, applications, and programs have become a growing concern for many computer users. This has led to a gradual yet steady rise in the installation and usage of alternative software such as the Tor browser, which purports to be able to prevent others from uncovering the true location of the end user. However, even these methods are not impervious to forensic investigation, as demonstrated at the **Digital Forensics Research Workshop 2015 by Epifani et al.**

Any attempt at obfuscation or extensive deletion of data should spark a level of suspicion in the mind of an investigator; anti-forensic methods are becoming more and more widespread, but so in turn are the methods forensic analysts can use to uncover the elements users were trying to hide.

Ensuring evidence is forensically sound

The chain of custody in digital investigations is of paramount importance. Not only does it demonstrate who had access to the evidence at any given time, it also - at least in theory - shows what was done with the evidence after it was seized, and the measures that were taken to ensure its preservation and integrity.

For investigators who work in a team, for example in law enforcement agencies or within a corporation, there will generally be an already established process to follow, in line with the guidelines provided by the agency or company. For freelance and individual investigators (or for those who believe their company's acquisition procedure may need a bit of an overhaul), it is important to bear a few basic principles in mind.

The level of forensic soundness that you as an investigator will be required to demonstrate will probably depend, at least in part, on the nature of the case on which you are working. Civil cases, for example, will generally not require such a high level of evidential integrity as criminal investigations, since civil cases are less likely to end up in court. It is good practice, however, to get used to maintaining as high a level of forensic soundness as possible;"doing so means that, if in the future you specialize in more in-depth investigations, you will already you will already be used to setting the right level of groundwork for your forensic examinations.

Generally, it is sufficient when gathering evidence to image a device—that is, to create an exact copy of the data contained therein—and then to use this forensic image as the basis for your analysis, rather than conducting analysis on the physical device you have seized from the scene. Sometimes, you may also be required to verify both that the copy is authentic, and that the process you used to copy the data did not alter it in any way. Audit trails are a large part of this—if you can demonstrate where the data sources have been stored, in which devices, for how long, and who has had access to them, this should suffice.

Removing the source of digital evidence from the scene of the investigation is the first step in this process and must be done with care. Switching off or unplugging a machine, typing in a password, moving a mouse, or performing any other kind of interaction with an object encountered in the course of a crime scene investigation can have unpredictable effects on the outcome of the investigation. Sometimes, devices are set up to be wiped automatically when turned off; some will encrypt all data when a password is entered incorrectly.

In most cases, investigators will be encouraged to leave the source of evidence in the state in which it is found. For example, if a mobile phone is recovered from a scene, it may be placed in a Faraday bag, which will block electric fields and therefore prevent signals from coming through while the phone is being transported.

If there is no way to remove an item from a scene without somehow tampering with it—for example, if a desktop PC is plugged in and turned on, but needs to be taken away for analysis—the person tasked with the removal of the item should be expertly qualified to ensure that no changes happen except the ones that are absolutely necessary, and that any actions that take place are detailed within the audit trail.

It may sound like this is a relatively straightforward process—don't change anything unless you absolutely have to; if you do have to, ensure the person who is making the changes is qualified to do so; and keep a record of everything that happens. However, this is a broad overview of the basic general requirements for the sound preservation of evidence, and these will differ—sometimes quite widely—depending on local or national legislation. One of the most challenging things about being a specialist in computer forensics is that computer crimes often have an international flavor, and it is not unheard of for an investigation to span several continents, let alone states within a given country.

For this reason, it is of the utmost importance to verify the local legislative requirements when it comes to the identification, collection, preservation, and analysis of digital forensic evidence, particularly if the case on which you are working is likely to end up in court.

Writing reports

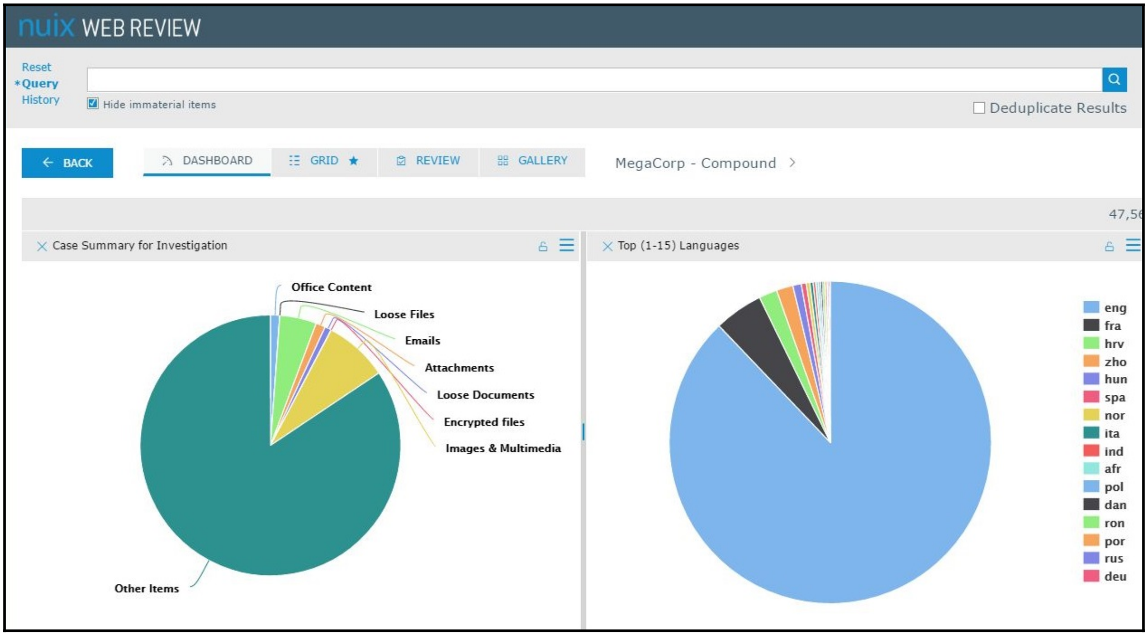
As with the chain of custody/audit trail mentioned in the preceding section, the style of report writing will no doubt vary based on legislative demands, company or agency guidelines, and individual investigator style. Once again, it makes sense to have a good grounding in the basics of digital forensic report writing, so that you have a flexible skill set within which to work.

Reports may also differ significantly depending on who is going to end up reading them. If you are investigating a civil dispute, your final report will probably not be written in highly technical language and may just include an overview in layperson terms of the methodology used and what was uncovered. If you are going to be called into court as an expert witness however, then a higher level of technical detail and a more in-depth demonstration of your investigative processes will no doubt be needed.

Broadly speaking, most digital evidence reports should include the following:

- Name, job title, and company of the senior investigating officer.
- Name, job title, and company of the digital forensics examiner (if different from the preceding one).
- A brief description of the case, including the nature of the activities under investigation.
- Name of the person or persons whose devices or data are under investigation.
- Start and end date of the investigation.
- Methodology used throughout the investigation, including but not limited to how evidence was identified, collected, preserved, and analyzed. This may also include details of any tools and processes used, as well as a copy of the chain of custody.
- An overview of the results of the investigation in line with the original activities specified at the beginning of the report, as well as any other relevant information that was uncovered in the course of the investigation.
- Screenshots, printouts, or other evidential items that demonstrate the results of the case.
- An analysis of the results, including any conclusions regarding guilt or innocence of the accused party.
- Any appendices, glossaries, or other information that may prove useful to the reader of the report.

Many forensic tools will generate their own reports in either digital or printable formats, in a number of different styles such as PDFs, Excel documents, or Word files. Some software packages, such as Nuix's Investigator Suite, include add-ons like Web Review and Analytics, which allow for multiple users to view or work on the same case. This can be very useful during an investigation, as it allows an administrator or senior investigator to allocate certain roles within a case, but it can also come in handy when compiling reports. Some users can be given access only to the final report, which they can enter into and look at the results that have been found and compiled into user-friendly graphs; if they have the correct permissions, they can then also take a further look at the evidence from this. The following diagram shows the dashboard of the Nuix Web Review and Analytics interface, which allows users to view and manage evidence in a forensic investigation.



Digital forensic investigation - an international field

As we have briefly discussed, one of the biggest challenges encountered by digital forensic investigators, whether in criminal or civil cases is the international nature of their investigative scope.

When investigating cases such as **DDoS** attacks (where a person or group of people flood a website or machine with requests in order to stop it from functioning), online credit card details theft, or bank fraud for example, it is likely that an investigator may find their suspects scattered all around the world. In a recent case involving the live streaming of child abuse from the Philippines, one of the main problems the investigators ran into was that the people who were watching the live streamed content were also subjects for investigation, but they were spread internationally and were difficult to track down due to so many of them using various methods of obfuscation. Laws around the world differ too: legislation in one country may create a legal loophole that causes havoc for a case and has implications on whether it is eventually brought to a conclusion or shelved.

The increasingly globalised nature of crime means that this is a problem we cannot ignore - it is not something that is going to go away. On the contrary, it looks set to only grow further with each passing year. Nowadays, our data is stored in the cloud—Nowadays, our data is stored in the cloud; people we interact with aren't just those we have met in real life, but instead people we would have previously termed strangers now increasingly form the basis of our social interactions; our bank accounts are accessible from almost anywhere in the world, often in multiple currencies. It is difficult enough to trace the actions and data trail of a single individual who is merely living life in the 21st century, let alone to attempt to investigate a large group of people, spread across diverse physical locations, who are making deliberate and sustained attempts to obfuscate data and hide themselves from view.

Strides ahead are being made, however. Various projects have sprung up over recent years which aim to address the specific challenges brought up by international investigations. One example is the EVIDENCE Project coordinated by Maria Angela Biasotti, an Italian lawyer who, in collaboration with colleagues across Europe, is seeking to develop a common understanding of electronic evidence and a more globally viable way of collaborating between territories, as well as a more standardized criminal investigation procedure around the world.

A laudable goal, and one that the EVIDENCE Project at least is moving swiftly towards; at the time of writing, a test implementation between several member countries is on the cards. However, at the moment, investigators are still faced with having to work on cases that have international data sources and implications.

What can we do to make things easier for ourselves in the meantime?

Scoping out a case before taking it on is good practice regardless of its size or relative importance, but this becomes even more pertinent when international factors might be involved. These may have an impact on the time it takes to acquire evidence: for example, if you are looking to extract data from a server in another country, or even another state, you will need at least a basic understanding of the requirements necessary to gain access to it, and indeed whether this is even possible in the first place.

It is, of course, impossible to have an in-depth understanding of the various bits of legislation that are relevant to digital forensic investigations around the world. In reality, the best an investigator can do is to verse themselves as fully as possible in the laws of their own local area, and then seek advice when the need arises to work across borders.

Beyond the legislative elements, however, there are also the more mundane aspects of international investigation, such as linguistic analysis. Keyword searches are often where an investigation starts, or at least fall somewhere near the beginning—but if your case spans a multitude of countries, you may well end up at a loss for keywords.

Most of the larger digital forensics solutions, such as EnCase and **Nuix Investigator**, have multilingual keyword abilities built in, which is a huge help. Some can even scan the evidence you enter for you, and then bring back an analysis of the languages used within the case. You can then use this to form the basis of your investigation and to inform future searches. Slang is still a problem for many though, and criminals are increasingly becoming wise to this. While a thesaurus can bring back a number of synonyms for a given term relating to drug abuse, the exploitation of children, or financial fraud, it may not be able to include all the less formal terms people are using in their discussions.

Progress is being made, however, and much of the air time at digital forensics conferences and research groups is devoted to how we as investigators can increase collaboration and make it easier to investigate global cases.

Challenges of acquiring digital evidence from Windows systems

One of the challenges of investigating Windows machines is the way that NTFS is set up. This means that it can be difficult to work out whether what you're looking at refers to a general property of the file system, or to a property that is specific to an application. The further along in your investigative career you are of course, the more adept you will become at making such distinctions, however, it is worth bearing in mind particularly for early career investigators.

Beyond the basic filesystem challenges, the way in which Windows systems are constantly updating can bring up further obstacles to digital forensic investigations. What worked on a machine running Windows 7 may not work on one that's running Windows 8.1; Windows 10 is a minefield of new and intriguing forensic elements (not to mention the increased privacy concerns it has brought up, leading to a rise in the number of users who are implementing their own data obfuscation and personal privacy measures). And heaven forbid you end up with a machine so old that modern forensic software has forgotten how to analyze it!

The way Windows 10 runs is of particular interest to forensic examiners, not just because it is being forcibly rolled out to users everywhere, but also because the structure of how things are organised has changed significantly. We will look at this in more detail towards the end of this book, where a full chapter will be devoted to the forensic analysis of machines running Windows 10, but broadly speaking, the difference from a forensic perspective comes from the fact that applications and programs don't just have different names; they work in a slightly different way. End users are increasingly looking for more lightweight, quick to run devices that make their work and personal lives easier, which means that, in turn, technology companies such as Microsoft are turning to collaborations with other entities and making the personal computer less of a single, standalone piece of equipment and more of a portal to data stored elsewhere. It is quite possible to seize a device where the documents are stored on Google Drive; voice and video call communications on Skype; Instagram is an application accessed on the PC rather than - or as well as - on a smartphone; Facebook isn't a website visited via an internet browser but an application in its own right.

Notwithstanding the legal challenges concerning international cloud data storage that we have already discussed, having such a wealth of separate applications to analyze makes cases much more complex. The fact that users can also add or create their own programs makes for an increasingly complex and often labyrinthine investigative methodology.

For this reason, it is becoming more and more necessary to narrow down an investigation as quickly as possible, working out which kinds of applications and services a user may require to perform the activity for which they are being investigated. Again, this is not always easy to do; we can but try!

Triage, international collaboration, and the technical understanding of investigators are all of paramount importance to digital forensic investigations, now more than ever before. In the *Windows Forensics Cookbook*, we hope to give you a base upon which you can build your own investigative techniques.

1. `https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0`, accessed 07/02/2017
2. `https://dfrws.org/sites/default/files/session-files/pres-tor_forensics_on_windows_os.pdf`, accessed 09/02/2017
3. `https://articles.forensicfocus.com/2016/05/02/the-investigative-challenges-of-live-streamed-child-abuse/`, accessed 09/02/2017

2

Windows Memory Acquisition and Analysis

In this chapter, we will cover the following recipes:

- Windows memory acquisition with Belkasoft RAM Capturer
- Windows memory acquisition with DumpIt
- Windows memory image analysis with Belkasoft Evidence Center
- Windows memory image analysis with Volatility
- Variations in Windows versions

Introduction

Memory analysis is a relatively new, but increasingly relevant field. A memory image can be acquired in the same way as a physical image, but by using different tools, some of which will be discussed in this section.

The image can be stored as one of the many formats, depending on the tool used to acquire the image. Once an investigator has the image, they can then analyse the data within it.

One of the main challenges associated with memory forensics is data preservation. Although your only option in a given investigation may be to power down a system and then image the data therein, in reality this ends up having an impact on other potential data sources that might be important later on. It is vital, therefore, to have a thorough understanding of the scene you are investigating and the specific needs of the case before you decide which method to choose. Any time you interact with a system, you will alter something simply by virtue of having been there. However, memory acquisition can help to minimize the effects of the investigator on the data collected, since a memory image will sample the volatile memory at a specific time, thus creating a sort of snapshot that can then be analysed later.

In cases where an investigator arrives at a scene to find a machine powered on, the memory on the system will be volatile at that time. This means that, if you manage to acquire a memory image then and there, you will be able to see a snapshot of the computer's memory at the moment at which you acquired it. This can be very useful, especially if a suspect has recently fled a scene or has been arrested at the scene.

You will generally need administrative permissions on the computer if you want to acquire volatile memory unless you are using hardware. One such solution is **CaptureGUARD Physical Memory Acquisition Hardware.** It requires a small CaptureGUARD driver to be installed on the system and creates a memory dump in the standard WinDD format. You can see one of these devices in figure 2.1.

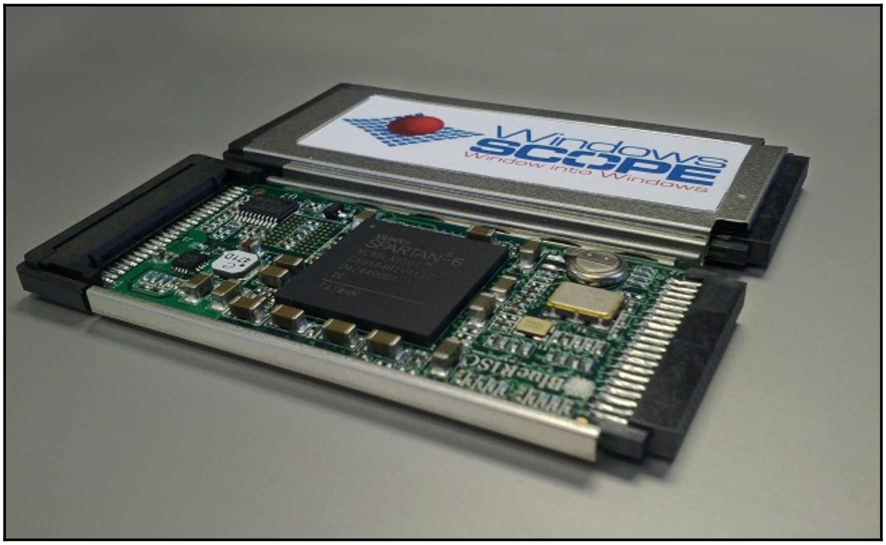


Figure 2.1. ExpressCard

In other words, memory forensics is a complex and temperamental field. You will need to have a thorough understanding of the tool sets you are using, and any potential impacts they could have on volatile memory before you decide which to use it at a scene. However, if you do manage to acquire a memory image, it can provide a wealth of useful information for your case.

Windows memory acquisition with Belkasoft RAM Capturer

Belkasoft RAM Capturer is a free tool any digital forensic examiner should have in their kit. It's tiny, easy to use, and has the ability to acquire memory from Windows systems, including Windows 10, even if they are protected by an active anti-debugging or anti-dumping system.

Getting ready

You have two options for downloading the tool. If you are a Belkasoft customer and have a Belkasoft Evidence Center license, go to your customer portal, where you can find a Belkasoft RAM Capturer download link in the **FREE PRODUCTS** section. If you are not a customer, just go to the **DOWNLOAD** section on the Belkasoft website, choose the product you want to download - in our case, Belkasoft Live RAM Capturer - and fill in a short form with your contact information. After the download, a link will be sent to the email provided.

The steps to prepare a flash drive for acquisition are as follows:

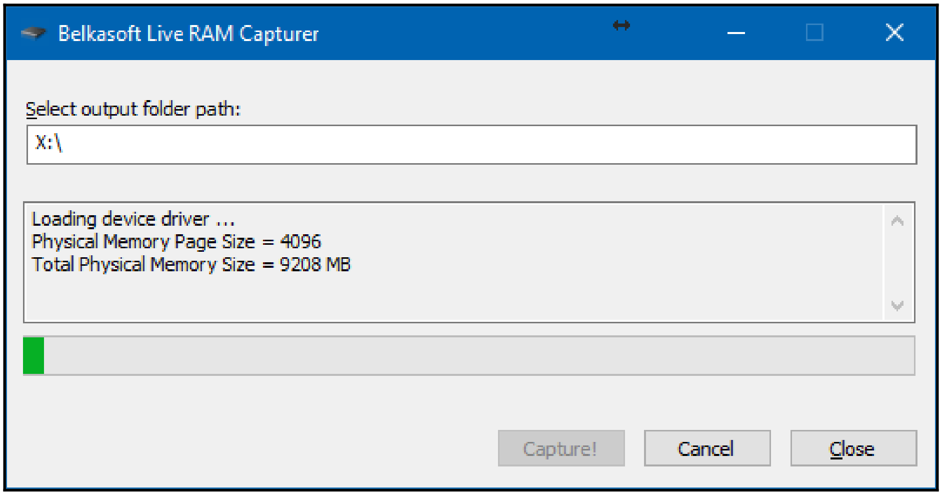
1. It must have enough space to store the memory image.
2. It must be sterilized via wiping.
3. Put both folders extracted from the archive you downloaded onto the flash drive.

Don't forget to prepare a flash drive for acquisition. Firstly, it must have enough space to store the memory image. Secondly, it must be sterilized by wiping. Finally, put both folders extracted from the archive you downloaded onto the flash drive.

How to do it…

The steps for Windows memory acquisition using Belkasoft Ram Capturer are as follows:

1. The first thing you must do is learn what kind of system you are dealing with – x32 or x64. It's really easy to do – right-click **Computer** and choose **Properties**. In our case, it's x64. So our choice is `RamCapture64.exe`.
2. After starting, we will get information about the physical memory page size and its total size.
3. Now select the output folder path – make sure it's your flash drive and not the local system drive.
4. After that – just click **Capture**!



Select output folder path: X:\

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 9208 MB
```

Figure 2.2. Memory acquisition with Belkasoft RAM Capturer

As a result, we get a file with `.mem` extension of the same size as the total physical memory. By default, you have the date of acquisition as the filename, but we highly recommend renaming it, and adding more information for identification purposes: operating system version, edition, computer name, and other information.

That's it! The image is ready for further analysis with memory forensics tools.

How it works…

Belkasoft RAM Capturer operates in kernel mode (not in user mode like some other acquisition tools) with the help of 32-bit and 64-bit kernel drivers. It extracts the whole physical memory, even if it's protected, in a forensically sound manner, and saves it into a file with the `.mem` extension.

See also

The Belkasoft RAM Capturer page on Belkasoft's website: `http://belkasoft.com/ram-capturer`

Windows memory acquisition with DumpIt

DumpIt is a free memory imaging tool from Comae Memory Toolkit. It's a fusion of Win32dd and Win64dd in one executable. It's extremely easy to use: even a non-technical person can use it in emergency situations. DumpIt supports all modern Windows versions, from XP to 10, both 32 and 64-bit. Also, the tool has a very important feature: it displays the Directory Table Base and the address of the debugging data structures during the acquisition process.

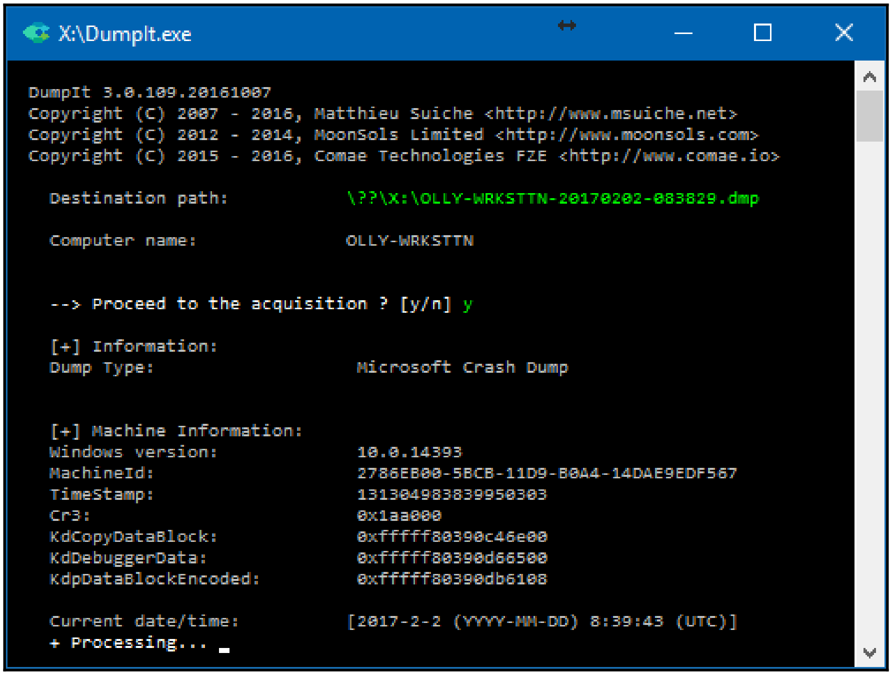
Getting ready

To get your free copy of DumpIt, go to Comae Technologies' website and click on **GET TOOLS**. After you provide some information, including your first name, last name, company name, email address, phone number and website, you'll get your download link via email. Don't forget to put the tool onto a wiped external drive later.

How to do it…

This time, we don't need to know what kind of operating system we are dealing with - 32 or 64-bit. As we have already been said, DumpIt is a fusion of Win32dd and Win64dd in one executable. So, there are just two steps:

1. Plug in the external drive in the target system
2. Start `DumpIt.exe` and type `y` to start the acquisition process



```
DumpIt 3.0.109.20161007
Copyright (C) 2007 - 2016, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2016, Comae Technologies FZE <http://www.comae.io>

  Destination path:           \??\X:\OLLY-WRKSTTN-20170202-083829.dmp

  Computer name:              OLLY-WRKSTTN


  --> Proceed to the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:             10.0.14393
  MachineId:                   2786EB00-5BCB-11D9-B0A4-14DAE9EDF567
  TimeStamp:                   131304983839950303
  Cr3:                         0x1aa000
  KdCopyDataBlock:             0xfffff80390c46e00
  KdDebuggerData:              0xfffff80390d66500
  KdpDataBlockEncoded:         0xfffff80390db6108

  Current date/time:          [2017-2-2 (YYYY-MM-DD) 8:39:43 (UTC)]
  + Processing... _
```

Figure 2.3. Memory acquisition with DumpIt

As a result of the acquisition, you'll get two files: a file with the DMP extension and a file with the JSON extension. The first is the target system's memory dump with the computer name, date and time (UTC) in the file name, the second - the dump information, includes important information from a forensic point of view. It includes file size, system architecture type (32/64), KdCopyDataBlock KdDebuggerData, kdpDataBlockEncoded, sha256 hash, and so on. So that's it, the DMP file is ready to be analysed with the memory forensics software of your choice.

How it works…

As DumpIt is a fusion of Win32dd and Win64dd, it automatically detects the system architecture type and creates a memory snapshot and a file in JSON format with all the information you will need for further analysis with memory forensics tools, such as Volatility, Rekall, Belkasoft Evidence Center, and others.

See also

The Comae Memory Toolkit (which DumpIt, along with Hibr2Bin, is a part of) webpage:

`https://comae.typeform.com/to/XIvMa7`

Windows memory image analysis with Belkasoft Evidence Center

In the previous recipes, we successfully created two memory forensic images, one with Belkasoft Live RAM Capturer, and the other with DumpIt. Now it's time to perform analysis. Let's start from the first image and use Belkasoft Evidence Center for analysis.

Belkasoft Evidence Center is a powerful digital forensics tool, capable of parsing data not only from memory images, but also from images of computer drives and mobile devices. From a memory dump, it can extract valuable artifacts such as remnants of communications via social networks, messengers, chat rooms, webmail systems, data from cloud services, web-browsing artifacts, and so on.

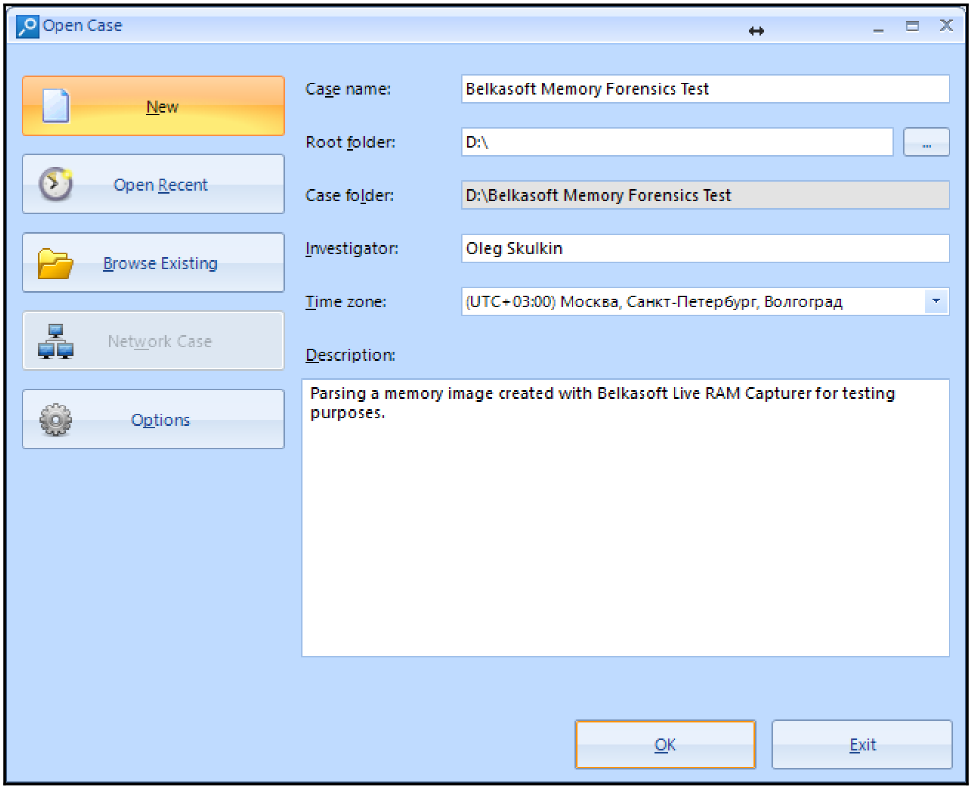
Getting ready

If you don't have a valid license for Belkasoft Evidence Center, you can download a fully functional trial version of the product from the official website. To do this, go to the **DOWNLOAD** section on Belkasoft's website, choose the product you want to download, in our case, Belkasoft Evidence Center (trial version) - and provide your **contact information**, including your F**irst Name**, L**ast Name**, **Your email** and **Company, Country**. After the download, the link will be sent to your email. If you are a licensed user, just go to your customer portal and download the latest version of the product.

How to do it...

The steps for Windows memory image analysis using Belkasoft Evidence Center:

1. To do that, click on **New** in the **Open Case** window. Now you need to fill in a few fields:
    - **Case name** - Usually, we use the case number and year for case names, but this time, as it's being created for testing purposes, we will name it `Belkasoft Memory Forensics Test`.
    - **Root folder** - Here, you should choose the folder where the case data will reside. In our case it's D: drive.
    - **Case folder** - This field will be filled in automatically based on the two previous fields, so in our case, it's `D:\Belkasoft Memory Forensics Test`.
    - **Investigator** - Type your name in this field.
    - **Time zone** - Choosing the right time zone is very important. If you already know the right one, choose it. If not, we suggest choosing UTC +00:00. In our case, we know the time zone, so we can use the correct one (UTC + 03:00).
    - **Description** - If you want to add a description to your digital evidence item, here is the field to do it. We used the following description: `Parsing a memory image created with Belkasoft Live RAM Capturer for testing purposes`.



Case name: Belkasoft Memory Forensics Test

Root folder: D:\

Case folder: D:\Belkasoft Memory Forensics Test

Investigator: Oleg Skulkin

Time zone: (UTC+03:00) Москва, Санкт-Петербург, Волгоград

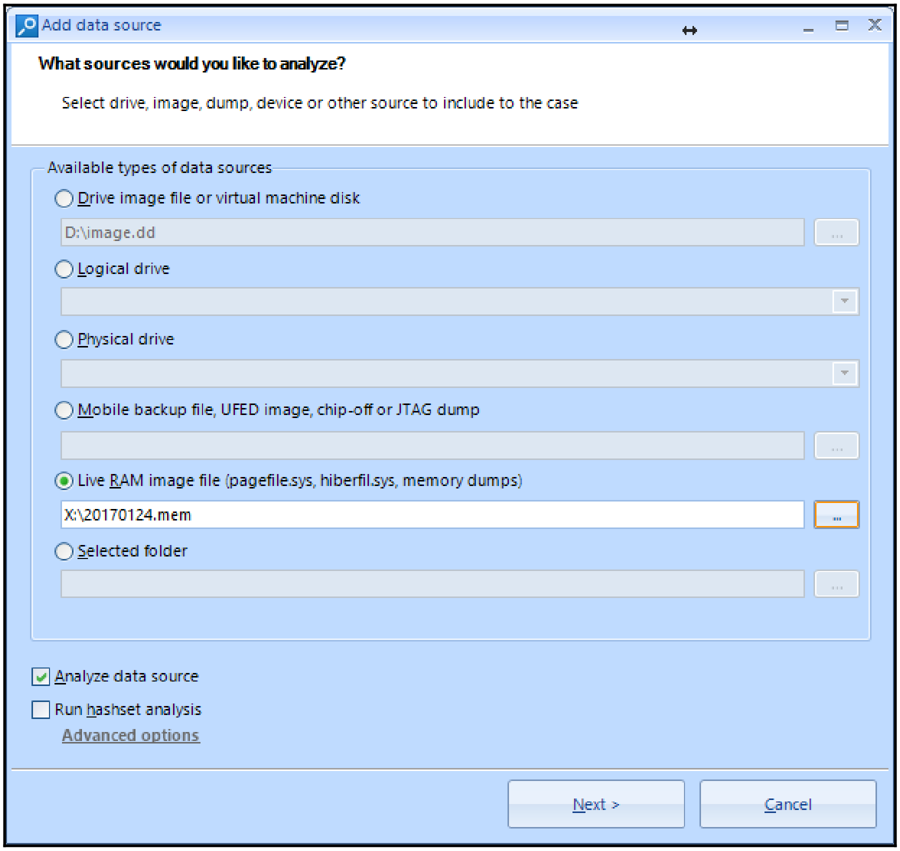
Description: Parsing a memory image created with Belkasoft Live RAM Capturer for testing purposes.

Figure 2.4. Creating a new case in Belkasoft Evidence Center

2. Click **OK** and you will see the next window - **Add data source**.

   Belkasoft Evidence Center supports different kinds of evidence sources, from physical drives and drive images, to mobile backups and, of course, memory images, including `pagefile.sys` and `hiberfil.sys`.

As we are talking about memory forensics now, let's choose the image we previously acquired with Belkasoft RAM Capturer as the data source.



Add data source

What sources would you like to analyze?

Select drive, image, dump, device or other source to include to the case

Available types of data sources

○ Drive image file or virtual machine disk

D:\image.dd

○ Logical drive

○ Physical drive

○ Mobile backup file, UFED image, chip-off or JTAG dump

● Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

X:\20170124.mem

○ Selected folder

☑ Analyze data source

□ Run hashset analysis

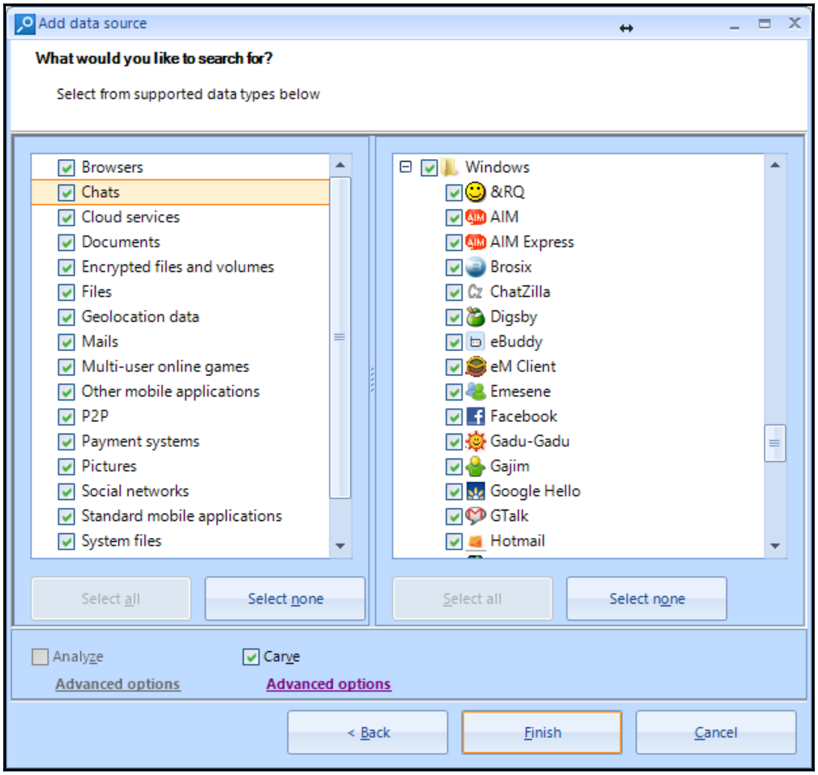
Advanced options

Figure 2.5. Adding previously acquired memory image as data source in Belkasoft Evidence Center

3. Click **Next** to choose the data types you want to search for. For testing purposes, we chose all available data types, but you can choose those you really need, to reduce processing time.

TIP

Don't forget to go to Advanced options and enable BelkaCarving - it will help you to recover fragmented data, for example, pictures.



Add data source

What would you like to search for?

Select from supported data types below

- ☑ Browsers
- ☑ Chats
- ☑ Cloud services
- ☑ Documents
- ☑ Encrypted files and volumes
- ☑ Files
- ☑ Geolocation data
- ☑ Mails
- ☑ Multi-user online games
- ☑ Other mobile applications
- ☑ P2P
- ☑ Payment systems
- ☑ Pictures
- ☑ Social networks
- ☑ Standard mobile applications
- ☑ System files

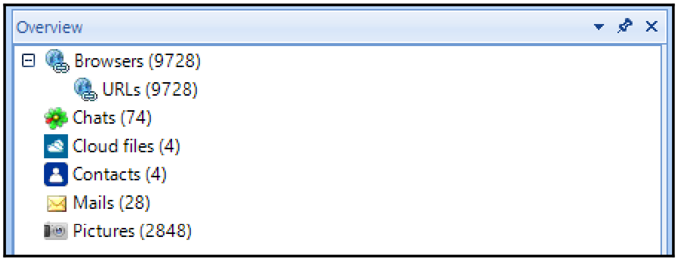
- ☑ Windows
  - ☑ &RQ
  - ☑ AIM
  - ☑ AIM Express
  - ☑ Brosix
  - ☑ ChatZilla
  - ☑ Digsby
  - ☑ eBuddy
  - ☑ eM Client
  - ☑ Emesene
  - ☑ Facebook
  - ☑ Gadu-Gadu
  - ☑ Gajim
  - ☑ Google Hello
  - ☑ GTalk
  - ☑ Hotmail

□ Analyze ☑ Carve

Figure 2.6. Choosing data types in Belkasoft Evidence Center

4. OK, we are ready to start parsing the memory image - just click **Finish**.

   It took BEC about an hour to parse and carve the image, and we got impressive results: 9728 web browser artifacts, 2848 pictures, 74 chat artifacts, and so on.



Overview

- Browsers (9728)
  - URLs (9728)
- Chats (74)
- Cloud files (4)
- Contacts (4)
- Mails (28)
- Pictures (2848)

Figure 2.7. Results of memory image processing with Belkasoft Evidence Center

As you can see, you can extract quite a lot of valuable digital artifacts from a memory image with just a few clicks - so, if you have access to a running system, make it a rule to capture the memory image. This may help you, for example, to recover browsing history from anonymous tools such as Tor Browser, which are widely used among criminals, as well as other important digital artifacts which may reside only in volatile memory.

How it works...

Belkasoft Evidence Center parses memory image structure and extracts available data, putting it into corresponding categories. The BelkaCarving options allow the tool to reconstruct fragmented data, for example, images.

See also

The Belkasoft Evidence Center page on the Belkasoft website: `http://belkasoft.com/ec`

BelkaCarving: `http://ru.belkasoft.com/en/bec/en/BelkaCarving.asp`

Windows memory image analysis with Volatility

The Volatility Framework is an open source collection of tools written in Python for the extraction of digital artifacts from memory images. This time, we will use the second memory image, obtained earlier with DumpIt, as a data source to show you how to use this tool set for memory forensics.

Getting ready

The Volatility Framework is an open source toolkit, so it's cross-platform, which means that you can use any operating system family you want - Windows, Linux, or mac OS. Of course, you can build these tools from source, but there are also so-called standalone executables for all the operating systems mentioned. As this cookbook is about forensic examination of Windows OS and the memory dump, what we are going to analyze is collected from Windows 10, and we are going to use the Windows Standalone Executable.

At the time of writing, the most recent version of Volatility is 2.6. With this version, support for Windows 10 (including 14393.447) improved, also support for Windows Server 2016, mac OS Sierra 10.12, and Linux with KASLR kernels was added.

To download the collection of tools, go to the Volatility Framework website and use the Releases tab to choose the most recent version, in our case 2.6. Now, all you need is to unzip **volatility_2.6_win64_standalone.zip** which you've just downloaded, and you are ready to go.

How to do it...

To show you the power of Volatility, we decided to use a memory image from a system infected with known malware - **Stuxnet**. Why? Because this memory image is freely available, so you can download it and use it for training.

Let's start by collecting information about our image.

1. To do this, start `cmd.exe`.
2. Change the directory to the one with the Volatility Standalone Executable, and use the `imageinfo` plugin:

```
volatility_2.6_win64_standalone.exe –f
X:stuxnet.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based
on KDBG
search...
Suggested Profile(s) : WinXPSP2x86,
WinXPSP3x86 (Instantiated    with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (X:stuxnet.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80545ae0L
```

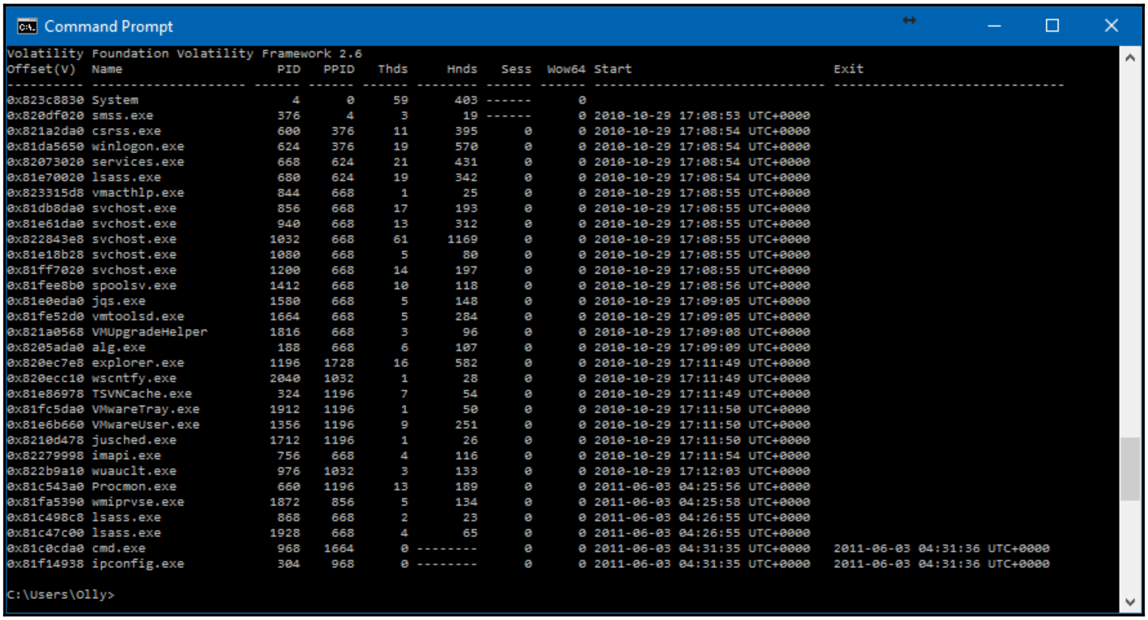
```
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdff000L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2011-06-03 04:31:36 UTC+0000
Image local date and time : 2011-06-03 00:31:36
-0400
```

The `imageinfo` plugin returned two suggested profiles. We know that this image was taken from a system running Windows XP with Service Pack 3, so the correct profile is WinXPSP3x86.

Now we know the correct profile, we can use it as a switch to collect information about the processes running on the infected machine.

3. To do this, we can use the `pslist` plugin:

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 pslist
```



```
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c8830 System                    4      0     59      403 ------      0
0x820df020 smss.exe                376      4      3       19 ------      0 2010-10-29 17:08:53 UTC+0000
0x821a2da0 csrss.exe               600    376     11      395      0      0 2010-10-29 17:08:54 UTC+0000
0x81da5650 winlogon.exe            624    376     19      570      0      0 2010-10-29 17:08:54 UTC+0000
0x82073020 services.exe            668    624     21      431      0      0 2010-10-29 17:08:54 UTC+0000
0x81e70020 lsass.exe               680    624     19      342      0      0 2010-10-29 17:08:54 UTC+0000
0x823315d8 vmacthlp.exe            844    668      1       25      0      0 2010-10-29 17:08:55 UTC+0000
0x81db8da0 svchost.exe             856    668     17      193      0      0 2010-10-29 17:08:55 UTC+0000
0x81e61da0 svchost.exe             940    668     13      312      0      0 2010-10-29 17:08:55 UTC+0000
0x822843e8 svchost.exe            1032    668     61     1169      0      0 2010-10-29 17:08:55 UTC+0000
0x81e18b28 svchost.exe            1080    668      5       80      0      0 2010-10-29 17:08:55 UTC+0000
0x81ff7020 svchost.exe            1200    668     14      197      0      0 2010-10-29 17:08:55 UTC+0000
0x81fee8b0 spoolsv.exe            1412    668     10      118      0      0 2010-10-29 17:08:56 UTC+0000
0x81e0eda0 jqs.exe                1580    668      5      148      0      0 2010-10-29 17:09:05 UTC+0000
0x81fe52d0 vmtoolsd.exe           1664    668      5      284      0      0 2010-10-29 17:09:05 UTC+0000
0x821a0568 VMUpgradeHelper        1816    668      3       96      0      0 2010-10-29 17:09:08 UTC+0000
0x8205ada0 alg.exe                 188    668      6      107      0      0 2010-10-29 17:09:09 UTC+0000
0x820ec7e8 explorer.exe           1196   1728     16      582      0      0 2010-10-29 17:11:49 UTC+0000
0x820ecc10 wscntfy.exe            2040   1032      1       28      0      0 2010-10-29 17:11:49 UTC+0000
0x81e86978 TSVNCache.exe           324   1196      7       54      0      0 2010-10-29 17:11:49 UTC+0000
0x81fc5da0 VMwareTray.exe         1912   1196      1       50      0      0 2010-10-29 17:11:50 UTC+0000
0x81e6b660 VMwareUser.exe         1356   1196      9      251      0      0 2010-10-29 17:11:50 UTC+0000
0x8210d478 jusched.exe            1712   1196      1       26      0      0 2010-10-29 17:11:50 UTC+0000
0x82279998 imapi.exe               756    668      4      116      0      0 2010-10-29 17:11:54 UTC+0000
0x822b9a10 wuauclt.exe             976   1032      3      133      0      0 2010-10-29 17:12:03 UTC+0000
0x81c543a0 Procmon.exe             660   1196     13      189      0      0 2011-06-03 04:25:56 UTC+0000
0x81fa5390 wmiprvse.exe           1872    856      5      134      0      0 2011-06-03 04:25:58 UTC+0000
0x81c498c8 lsass.exe               868    668      2       23      0      0 2011-06-03 04:26:55 UTC+0000
0x81c47c00 lsass.exe              1928    668      4       65      0      0 2011-06-03 04:26:55 UTC+0000
0x81c0cda0 cmd.exe                 968   1664      0 --------      0      0 2011-06-03 04:31:35 UTC+0000   2011-06-03 04:31:36 UTC+0000
0x81f14938 ipconfig.exe            304    968      0 --------      0      0 2011-06-03 04:31:35 UTC+0000   2011-06-03 04:31:36 UTC+0000

C:\Users\Olly>
```

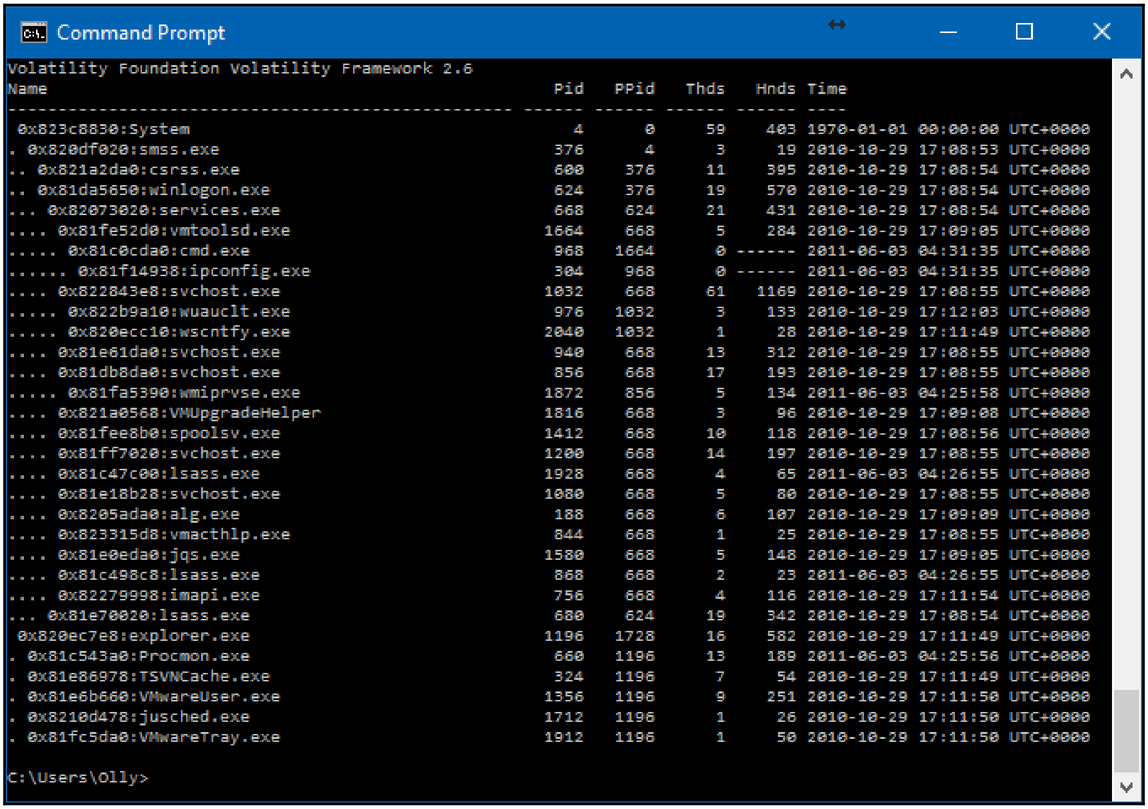
Figure 2.8. Volatility pslist plugin output

Do you see anything suspicious? Yes, there are three copies of `lsass.exe`, and this is one of the signs of a Stuxnet infection.

Normally, only one `lsass.exe` process should be running, so we need to determine which two are malicious.

4. Look at the timestamps on figure 2.8. Two out of three processes started in 2011. Strange, isn't it? Now let's use the `pstree` plugin:

```
volatility_2.6_win64_standalone.exe -f
X:stuxnet.vmem --
profile=WinXPSP3x86 pstree
```



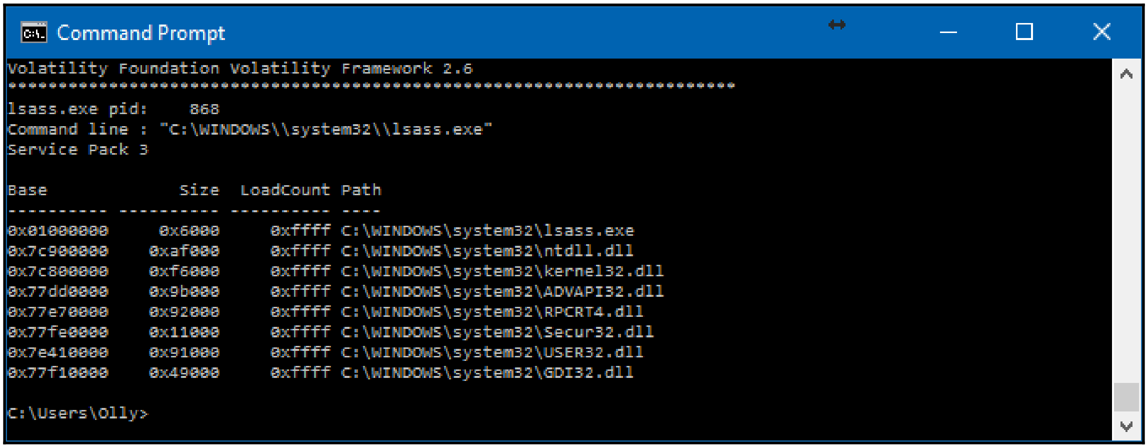
```
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     59    403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe                                 376      4      3     19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe                               600    376     11    395 2010-10-29 17:08:54 UTC+0000
.. 0x81da5650:winlogon.exe                            624    376     19    570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe                           668    624     21    431 2010-10-29 17:08:54 UTC+0000
.... 0x81fe52d0:vmtoolsd.exe                         1664    668      5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe                              968   1664      0 ------ 2011-06-03 04:31:35 UTC+0000
...... 0x81f14938:ipconfig.exe                        304    968      0 ------ 2011-06-03 04:31:35 UTC+0000
.... 0x822843e8:svchost.exe                          1032    668     61   1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuauclt.exe                          976   1032      3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe                         2040   1032      1     28 2010-10-29 17:11:49 UTC+0000
.... 0x81e61da0:svchost.exe                           940    668     13    312 2010-10-29 17:08:55 UTC+0000
.... 0x81db8da0:svchost.exe                           856    668     17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe                        1872    856      5    134 2011-06-03 04:25:58 UTC+0000
.... 0x821a0568:VMUpgradeHelper                      1816    668      3     96 2010-10-29 17:09:08 UTC+0000
.... 0x81fee8b0:spoolsv.exe                          1412    668     10    118 2010-10-29 17:08:56 UTC+0000
.... 0x81ff7020:svchost.exe                          1200    668     14    197 2010-10-29 17:08:55 UTC+0000
.... 0x81c47c00:lsass.exe                            1928    668      4     65 2011-06-03 04:26:55 UTC+0000
.... 0x81e18b28:svchost.exe                          1080    668      5     80 2010-10-29 17:08:55 UTC+0000
.... 0x8205ada0:alg.exe                               188    668      6    107 2010-10-29 17:09:09 UTC+0000
.... 0x823315d8:vmacthlp.exe                          844    668      1     25 2010-10-29 17:08:55 UTC+0000
.... 0x81e0eda0:jqs.exe                              1580    668      5    148 2010-10-29 17:09:05 UTC+0000
.... 0x81c498c8:lsass.exe                             868    668      2     23 2011-06-03 04:26:55 UTC+0000
.... 0x82279998:imapi.exe                             756    668      4    116 2010-10-29 17:11:54 UTC+0000
... 0x81e70020:lsass.exe                              680    624     19    342 2010-10-29 17:08:54 UTC+0000
 0x820ec7e8:explorer.exe                             1196   1728     16    582 2010-10-29 17:11:49 UTC+0000
. 0x81c543a0:Procmon.exe                              660   1196     13    189 2011-06-03 04:25:56 UTC+0000
. 0x81e86978:TSVNCache.exe                            324   1196      7     54 2010-10-29 17:11:49 UTC+0000
. 0x81e6b660:VMwareUser.exe                          1356   1196      9    251 2010-10-29 17:11:50 UTC+0000
. 0x8210d478:jusched.exe                             1712   1196      1     26 2010-10-29 17:11:50 UTC+0000
. 0x81fc5da0:VMwareTray.exe                          1912   1196      1     50 2010-10-29 17:11:50 UTC+0000

C:\Users\Olly>
```

Figure 2.9. Volatility pstree plugin output

Our suspicious process, `lsass.exe`, is normally started by `winlogon.exe`.

5. Let's look at the figure: only one `lsass.exe` is started by `winlogon.exe` - the one with PID 680; the two others are started by `services.exe`! So, the `lsass.exe` processes with PIDs `868` and `1928` could be malicious.
6. We have two potentially malicious processes. Let's check the DLLs loaded by these processes using the `dlllist` plugin:

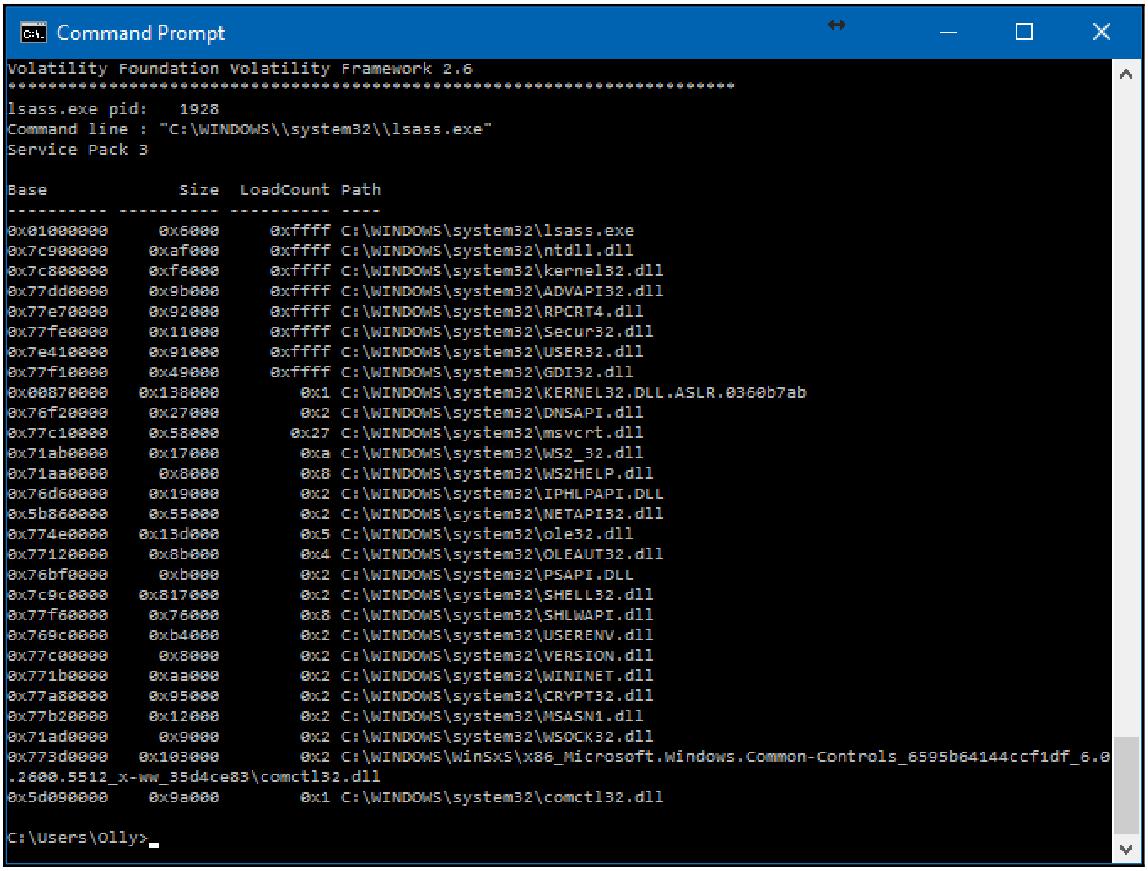
```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 -p 868
```



```
Volatility Foundation Volatility Framework 2.6
************************************************************************
lsass.exe pid:    868
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll

C:\Users\Olly>
```

Figure 2.10. Volatility dlllist plugin output for the suspicious process with PID 868

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
profile=WinXPSP3x86 -p 1928
```



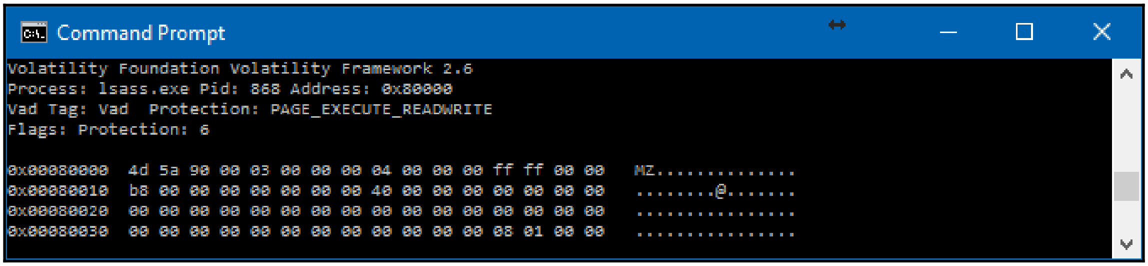
```
Volatility Foundation Volatility Framework 2.6
************************************************************************
lsass.exe pid:   1928
Command line : "C:\WINDOWS\\system32\\lsass.exe"
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x01000000     0x6000     0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll
0x00870000   0x138000        0x1 C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360b7ab
0x76f20000    0x27000        0x2 C:\WINDOWS\system32\DNSAPI.dll
0x77c10000    0x58000       0x27 C:\WINDOWS\system32\msvcrt.dll
0x71ab0000    0x17000        0xa C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000        0x8 C:\WINDOWS\system32\WS2HELP.dll
0x76d60000    0x19000        0x2 C:\WINDOWS\system32\IPHLPAPI.DLL
0x5b860000    0x55000        0x2 C:\WINDOWS\system32\NETAPI32.dll
0x774e0000   0x13d000        0x5 C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76bf0000     0xb000        0x2 C:\WINDOWS\system32\PSAPI.DLL
0x7c9c0000   0x817000        0x2 C:\WINDOWS\system32\SHELL32.dll
0x77f60000    0x76000        0x8 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000    0xb4000        0x2 C:\WINDOWS\system32\USERENV.dll
0x77c00000     0x8000        0x2 C:\WINDOWS\system32\VERSION.dll
0x771b0000    0xaa000        0x2 C:\WINDOWS\system32\WININET.dll
0x77a80000    0x95000        0x2 C:\WINDOWS\system32\CRYPT32.dll
0x77b20000    0x12000        0x2 C:\WINDOWS\system32\MSASN1.dll
0x71ad0000     0x9000        0x2 C:\WINDOWS\system32\WSOCK32.dll
0x773d0000   0x103000        0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0
.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll

C:\Users\Olly>_
```

Figure 2.11. Volatility dlllist plugin output for the suspicious process with PID 1928

7. Look at figure 2.11. Anything suspicious? Yes! According to the Stuxnet threat description on F-Secure's website, an encrypted DLL file should be injected into a process, and it has the following name structure: `[normaldll].ASLR.[random]`.
8. Look familiar? We have found another trace of Stuxnet - `KERNEL32.DLL.ASLR.0360b7ab`.

There is another extremely useful Volatility plugin - `malfind`. This plugin helps digital forensic examiners to find hidden or injected code/DLLs in the user mode memory. Let's use it for our suspicious `lsass.exe` processes:

```
volatility_2.6_win64_standalone.exe -f X:stuxnet.vmem
--
profile=WinXPSP3x86 malfind -p 868 --dump-dir
X:Stuxnet
```



```
Volatility Foundation Volatility Framework 2.6
Process: lsass.exe Pid: 868 Address: 0x80000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00080000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00080010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00080020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00080030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00   ................
```

Figure 2.12. A part of Volatility malfind plugin output for the suspicious process with PID 868

As you can see, we also used the `--dump-dir` switch to export the DLLs to a folder. After that we can, for example, upload them to VirusTotal. And of course, most of them are detected as malicious. For example, `process.0x81c47c00.0x80000.dmp`, extracted from `lsass.exe` with PID `1928`, is detected by Dr.Web Antivirus as **Trojan.Stuxnet.1**.

There are many more Volatility plugins available. You can learn more about them in the documentation available on the Volatility Foundation website.

How it works...

The following list explains the plugins used in the recipe.

1. `Imageinfo`: This plugin collects some basic information about the memory image you are analyzing: operating system, service pack, hardware architecture; and also useful information such as DTB address, KDBG address, and the timestamp of the image creation.

2. `Pslist`: This plugin shows the processes of the system, including the offset, process name, process ID, parent process ID, number of threads, number of handles, date/time when the process started and exited, Session ID and if the process is a WoW64 process.
3. `Pstree`: This plugin does the same as `pslist`, but shows the process list in tree form. It uses indentation and periods to indicate child processes.
4. `Dlllist`: This plugin displays the DLLs loaded by the process of interest, or all processes if the `-p` or `--pid` switch isn't used.
5. `Malfind`: This plugin allows the examiner to detect and extract hidden or injected code/DLLs in user mode memory for further antivirus scans and analysis.

See also

Volatility documentation: `https://github.com/volatilityfoundation/volatility/wiki`

A memory image from a system infected with Stuxnet: `https://github.com/ganboing/malwarecookbook`

Stuxnet threat description: `https://www.f-secure.com/v-descs/trojan-dropper_w32_stuxnet.shtml`

Variations in Windows versions

As you already know from the first chapter, nowadays we have a number of different Windows versions widely used both by private persons and businesses. Of course, this has an impact on Windows operating system forensic examinations, including Windows memory forensics.

Getting ready

Knowing the Windows version and its type is very important, both in the acquisition and analysis stages. There are a few ways to collect this information. We will cover some in this recipe.

How to do it...

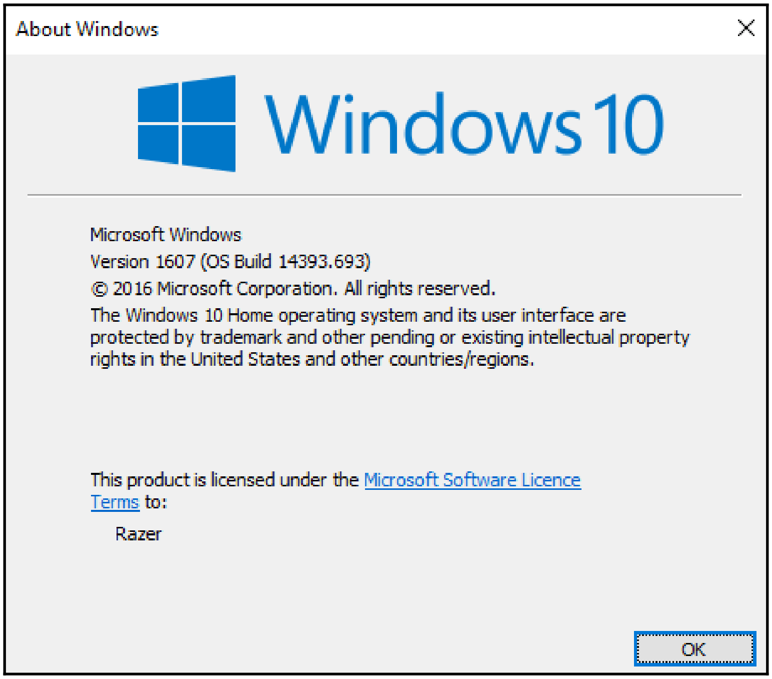
The easiest way to find out which version a computer is running is by following these steps:

1. Click on **Start**.
2. Go to **Run**.
3. Type `winver` in the search field and press *Enter*.

This will work on machines that have installed Windows 7 or earlier versions. For Windows 8 onwards:

1. You will need to press and hold the *Windows* key along with *R*
2. Type `winver` in the box that appears and press *Enter*

This will open a small **About Windows** box, which will provide information on the version, as well as the build number:



Microsoft Windows
Version 1607 (OS Build 14393.693)
© 2016 Microsoft Corporation. All rights reserved.
The Windows 10 Home operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software Licence Terms to:

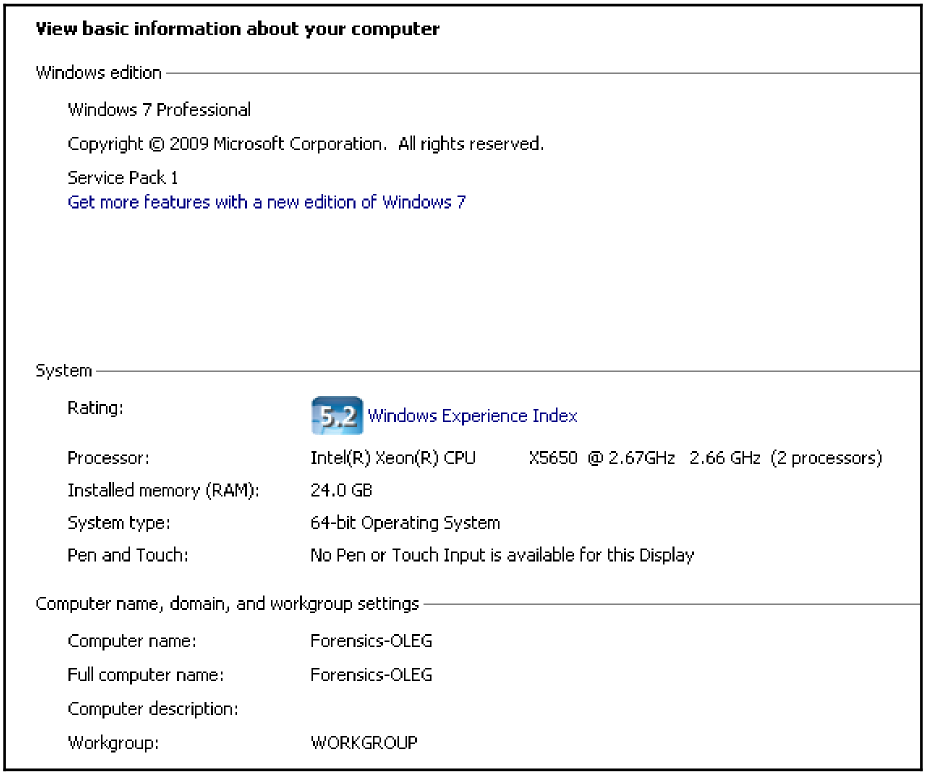
Razer

Figure 2.13. About Windows box

To collect more information, perform the following steps:

1. Go to the **Start** menu
2. Right-click on **Computer** and choose **Properties** from the context menu

   Also, you can find **My Computer**, **Computer**, or **This PC** shortcuts on the Desktop – right-click on any one of these and choose **Properties** from the context menu:



View basic information about your computer

Windows edition

Windows 7 Professional

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1
Get more features with a new edition of Windows 7

System

Rating:	5.2 Windows Experience Index
Processor:	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz 2.66 GHz (2 processors)
Installed memory (RAM):	24.0 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	Forensics-OLEG
Full computer name:	Forensics-OLEG
Computer description:	
Workgroup:	WORKGROUP

Figure 2.14. Computer properties

As you can see in figure 2.14, with this technique you can collect more information about the machine you are dealing with, including the service pack, **system type**, **computer name**, and so on.

There is more...

If you are planning to use Volatility for memory forensic analysis (and we highly recommend it, because it is the most powerful tool, with lots of plugins, and also it is free and open source), it's very important to choose the right profile. To do this, you will need to know the system type, operating system version, and build number. As you have already learned from the previous recipes, the `imageinfo` plugin can help you with this task if this information wasn't properly documented during the acquisition stage.

Table 2.1 contains information about profiles added to the most recent version of the Volatility Framework at the time of writing.

OS	**Build**	**Profile**
Windows 10 x64	**10.0.10586.306**	**Win10x64_10586**
Windows 10 x64	10.0.14393.0	Win10x64_14393
Windows 10 x86	10.0.10586.420	Win10x86_10586
Windows 10 x86	10.0.14393.0	Win10x86_14393
Windows Server 2008 R2 SP1 x64	6.1.7601.23418	Win2008R2SP1x64_23418
Windows Server 2008 R2 x64	6.3.9600.18340	Win2012R2x64_18340
Windows 7 SP1 x64	6.1.7601.23418	Win7SP1x64_23418
Windows 7 SP1 x86	6.1.7601.23418	Win7SP1x86_23418
Windows 8 x64	6.3.9600.18340	Win8SP1x64_18340

Table 2.1. Volatility 2.6 profiles list

Also, it's important to note that on all x64 Windows 8/2012 (and later), the KDBG (which contains a list of the running processes and loaded kernel modules) is encrypted by default, so you should use the virtual address of KdCopyDataBlock. Both addresses can be collected with the **kdbgscan** Volatility plugin.

3

Windows Drive Acquisition

In this chapter, we will cover the following recipes:

- Drive acquisition in E01 format with FTK Imager
- Drive acquisition in RAW format with dc3dd
- Mounting forensic images with Arsenal Image Mounter

Introduction

Before you can begin analysing evidence from a source, it first of all needs to be imaged. This describes a forensic process in which an exact copy of a drive is made. This is an important step, especially if evidence needs to be taken to court, because forensic investigators must be able to demonstrate that they have not altered the evidence in any way.

The term *forensic image* can refer to either a physical or a logical image. Physical images are precise replicas of the drives they reference, whereas a logical image is a copy of a certain volume within that drive. In general, logical images show what the machine's user will have seen and dealt with, whereas physical images give a more comprehensive overview of how the device works at a higher level.

A *hash value* is generated to verify the authenticity of the acquired image. Hash values are essentially cryptographic digital fingerprints which show whether a particular item is an exact copy of another. Altering even the smallest bit of data will generate a completely new hash value, thus demonstrating that the two items are not the same. When a forensic investigator images a drive, they should generate a hash value for both the original drive and the acquired image. Some pieces of forensic software will do this for you.

There are a number of tools available for imaging hard drives, some of which are free and open source. However, the most popular way for forensic analysts to image hard drives is by using one of the more well-known forensic software vendors' solutions. This is because it is imperative to be able to explain how the image was acquired and its integrity, especially if you are working on a case that will be taken to court.

Once you have your image, you will then be able to analyze the digital evidence from a device without directly interfering with the device itself.

In this chapter, we will be looking at various tools that can help you to image a Windows drive, and taking you through the process of acquisition.

Drive acquisition in E01 format with FTK Imager

FTK Imager is an imaging and data preview tool by AccessData which allows an examiner not only to create forensic images in different formats, including RAW, SMART, E01, and AFF, but also to preview data sources in a forensically sound manner. In the first recipe of this chapter, we will show you how to create a forensic image of a hard drive from a Windows system in E01 format.

E01 or EnCase's Evidence File is a standard format for forensic images in law enforcement. Such images consist of a header with case info, including acquisition date and time, examiner's name, acquisition notes, and password (optional), a bit-by-bit copy of an acquired drive (consisting of data blocks, verified with its own CRC or Cyclical Redundancy Check), and a footer with MD5 hash for the bitstream.

Getting ready

First of all, let's download **FTK Imager** from AccessData's website. To do this, go to the Products and Services tab, and after that, to **Product Downloads**. Now choose DIGITAL FORENSICS, and then **FTK Imager**. At the time of writing, the most up-to-date version is 3.4.3, so click the green **DOWNLOAD PAGE** button on the right. Now you should be able to see the download page. Click on **DOWNLOAD NOW** and fill in the form. After this, the download link will be sent to the email address that you provided.

The installation process is quite straightforward; all you need to do is just click **Next** a few times, so we won't cover it in the recipe.

How to do it...

There are two ways of initiating the drive imaging process:

1. Using the **Create Disk Image** button from the toolbar (Figure 3.1)

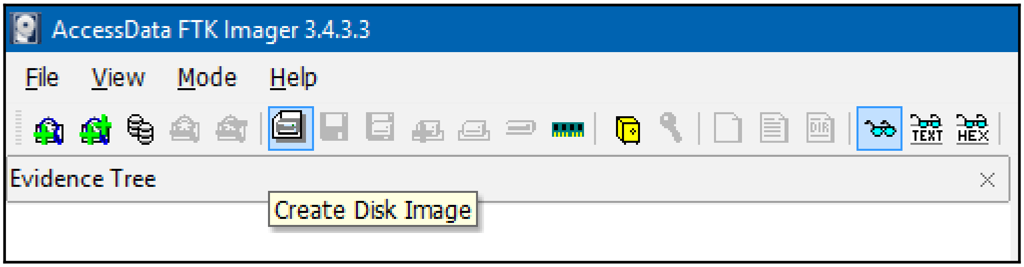


Figure 3.1. Create Disk Image button on the toolbar

2. Using the **Create Disk Image...** option from the **File** menu (Figure 3.2)

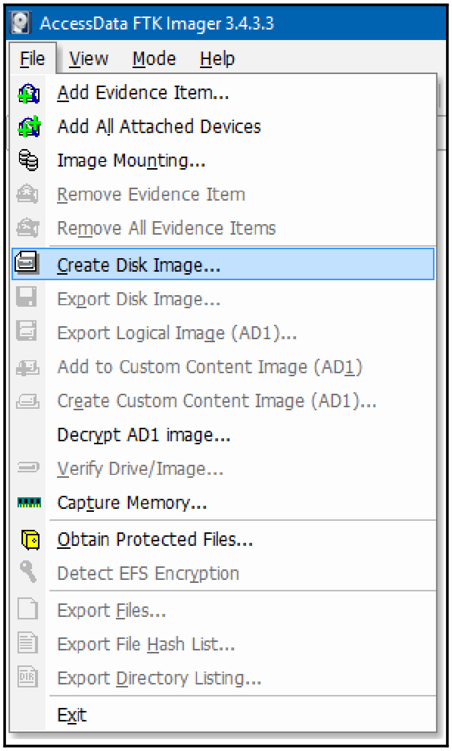


Figure 3.2. Create Disk Image... option in the File Menu

You can choose whichever option you prefer.

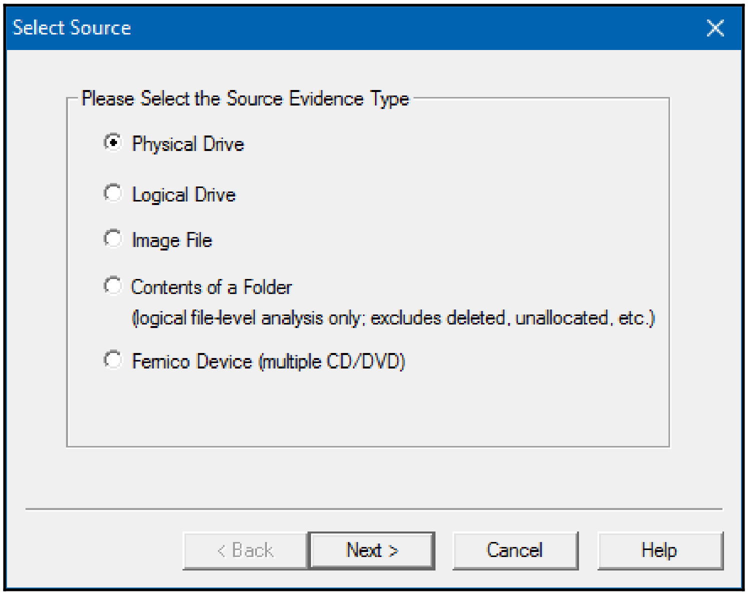
The first window you see is **Select Source**. Here, you have five options:

- **Physical Drive**: This allows you to choose a physical drive as the source, with all partitions and unallocated space.
- **Logical Drive**: This allows you to choose a logical drive as the source, for example `E:\ drive`.
- **Image File**: This allows you to choose an image file as the source, for example, if you need to convert your forensic image from one format to another.
- **Contents of a Folder**: This allows you to choose a folder as the source. Of course, no deleted files will be included.
- **Fernico Device**: This allows you to restore images from multiple CD/DVDs.

Of course we want to image the whole drive to be able to work with deleted data and unallocated space, so:

1. Let's choose the **Physical Drive** option.

> The evidence source mustn't be altered in any way, so make sure you are using a hardware write blocker. You can use the one from Tableau, for example. These devices allow acquisition of drive contents without creating the possibility of modifying the data.


Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

○ Image File

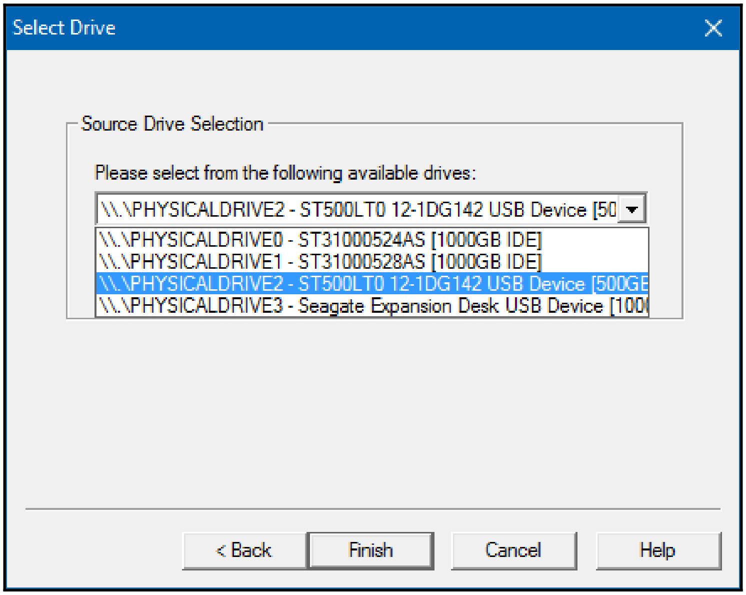
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

Figure 3.3. FTK Imager Select Source window

2. Click **Next** and you'll see the next window - **Select Drive**.

3. Now you should choose the source drive from the drop-down menu, in our case it's \\.**PHYSICALDRIVE2**.



Select Drive

Source Drive Selection

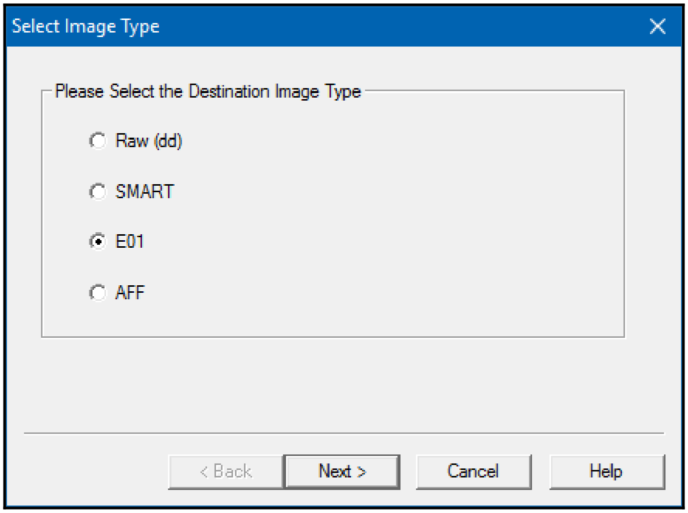
Please select from the following available drives:

\\.\PHYSICALDRIVE2 - ST500LT0 12-1DG142 USB Device [50

\\.\PHYSICALDRIVE0 - ST31000524AS [1000GB IDE]
\\.\PHYSICALDRIVE1 - ST31000528AS [1000GB IDE]
\\.\PHYSICALDRIVE2 - ST500LT0 12-1DG142 USB Device [500GE
\\.\PHYSICALDRIVE3 - Seagate Expansion Desk USB Device [100(

Figure 3.4. FTK Imager Select Drive window

4. Now that the source drive has been chosen, click **Finish**.
5. The next window is - **Create Image**. We'll get back to this window soon, but for now, just click **Add...**
6. It's time to choose the destination image type. As we decided to create our image in EnCase's Evidence File format, let's choose **E01**.



Please Select the Destination Image Type

○ Raw (dd)

○ SMART

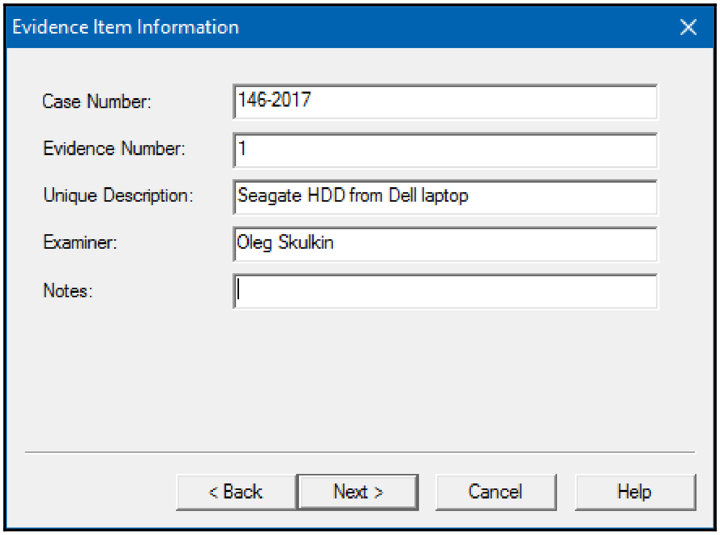
● E01

○ AFF

Figure 3.5. FTK Imager Select Image Type window

7. Click **Next** and you'll see the **Evidence Item Information** window.

   Here, we have five fields to fill in: **Case Number**, **Evidence Number**, **Unique Description**, **Examiner,** and **Notes**. All fields are optional.



Case Number:	146-2017
Evidence Number:	1
Unique Description:	Seagate HDD from Dell laptop
Examiner:	Oleg Skulkin
Notes:	

Figure 3.6. FTK Imager Evidence Item Information window

8. Fill in the fields, or skip them if you prefer, then click **Next.**
9. Now choose the image destination. You can use the **Browse** button for this.
10. Also, you should fill in the image filename.

If you want your forensic image to be split, choose a fragment size (in megabytes). E01 format supports compression, so if you want to reduce the image size, you can use this feature. As you can see in figure 3.7, we have chosen **6**. And if you want the data in the image to be secured, use the **AD Encryption feature**.

AD Encryption is a whole image encryption, so not only is the raw data encrypted, but so is any metadata. Each segment or file of the image is encrypted with a randomly generated image key using AES-256.

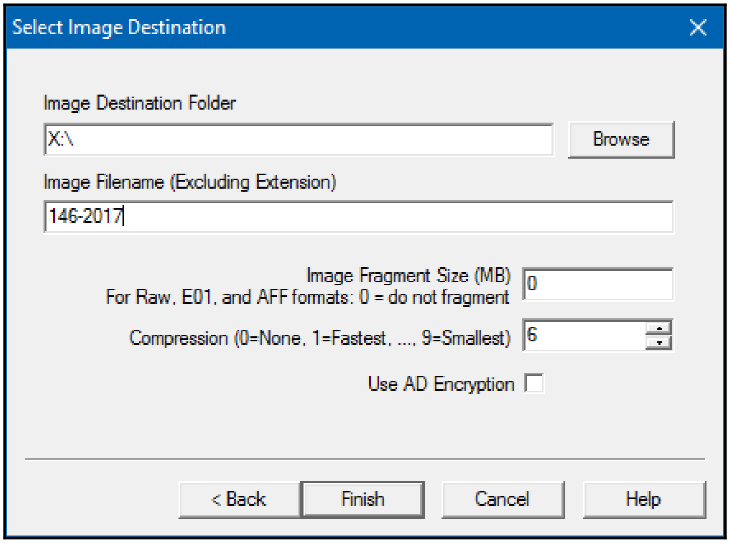


Image Destination Folder: X:\
Image Filename (Excluding Extension): 146-2017
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 0
Compression (0=None, 1=Fastest, ..., 9=Smallest): 6
Use AD Encryption ☐

Figure 3.7. FTK Imager Select Image Destination window

We are almost done.

11. Click **Finish** and you'll see the **Create Image** window again.
12. Now look at the three options at the bottom of the window.

The verification process is very important, so make sure the **Verify images after they are created** option is ticked; it helps you to be sure that the source and the image are equal. The **Precalculate Progress Statistics** option is also very useful: it will show you the estimated time of arrival during the imaging process. The last option will create directory listings of all files in the image for you, but of course, it takes time, so use it only if you need to.

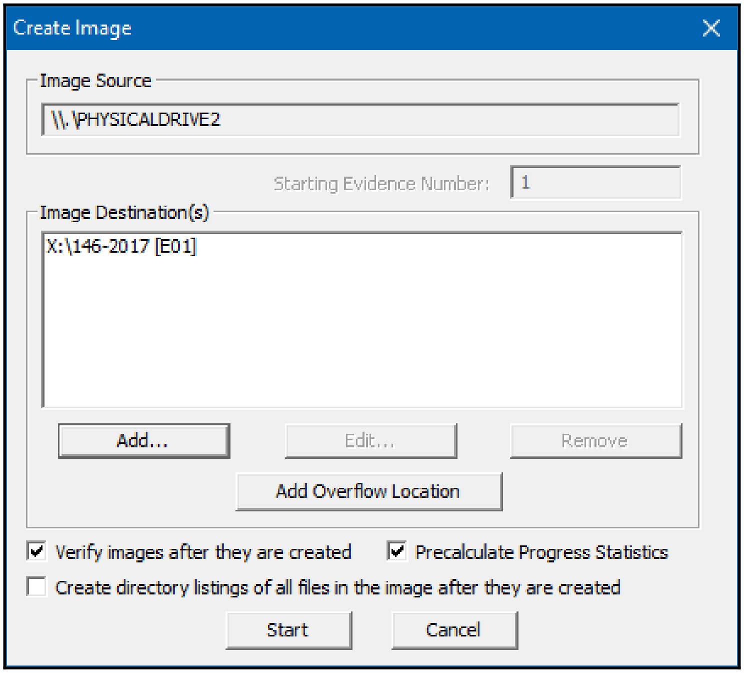

Create Image

Image Source: \\.\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s): X:\146-2017 [E01]

☑ Verify images after they are created ☑ Precalculate Progress Statistics

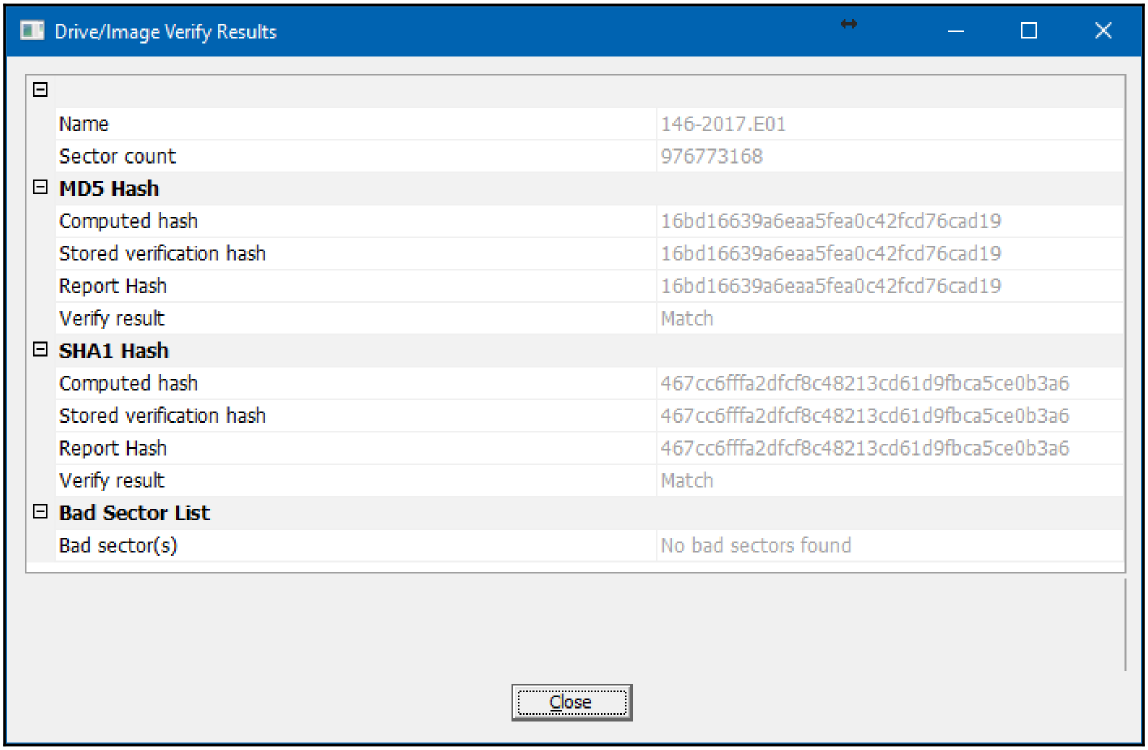
□ Create directory listings of all files in the image after they are created

Figure 3.8. FTK Imager Create Image window

13. All you need to do now is click **Start.**

Great, the imaging process has been started! Once the image has been created, the verification process starts.

14. Finally, you'll get a **Drive/Image Verify Results** window, like the one shown in figure 3.9.



Name	146-2017.E01
Sector count	976773168
MD5 Hash	
Computed hash	16bd16639a6eaa5fea0c42fcd76cad19
Stored verification hash	16bd16639a6eaa5fea0c42fcd76cad19
Report Hash	16bd16639a6eaa5fea0c42fcd76cad19
Verify result	Match
SHA1 Hash	
Computed hash	467cc6fffa2dfcf8c48213cd61d9fbca5ce0b3a6
Stored verification hash	467cc6fffa2dfcf8c48213cd61d9fbca5ce0b3a6
Report Hash	467cc6fffa2dfcf8c48213cd61d9fbca5ce0b3a6
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Figure 3.9. FTK Imager Drive/Image Verify Results window

As you can see, in our case the source and the image are identical: both hashes matched. In the folder with the image, you will also find an info file with valuable information such as the drive model, serial number, source data size, sector count, MD5 and SHA1 checksums, and so on.

How it works...

FTK Imager uses the physical drive of your choice as the source and creates a bit-by-bit image of it in EnCase's Evidence File format. During the verification process, MD5 and SHA1 hashes of the image and the source are compared.

See more

The FTK Imager download page:

```
http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.3
```

The FTK Imager User Guide:

```
https://ad-pdf.s3.amazonaws.com/Imager/3_4_3/FTKImager_UG.pdf
```

Drive acquisition in RAW format with dc3dd

DC3DD (by Jesse Kornblum) is a patched version of the classic GNU dd utility with some computer forensics features. For example, the fly hashing with a number of algorithms, such as MD5, SHA-1, SHA-256, and SHA-512, showing the progress of the acquisition process, and so on.

Getting ready

You can find a compiled standalone version of DC3DD for Windows at SourceForge. Just download the ZIP or 7z archive, unpack it, and you are ready to go.

How to do it...

The steps for drive acquisition in RAW format using dc3dd are as follows:

1. Open **Windows Command Prompt,** change directory (you can use **cd** command to do it) to the one with `dc3dd.exe`, and type the following command:

```
dc3dd.exe if=\\.\PHYSICALDRIVE2 of=X:\147-2017.dd hash=sha256
log=X:\147-2017.log
```

2. Press *Enter* and the acquisition process will start.

Of course, your command will be a bit different, so let's find out what each part of it means:

- **if** - stands for input file. Originally, dd was a Linux utility, and in case you didn't know, everything is a file in Linux. As you can see in our command, we put the physical drive 2 here (this is the drive we wanted to image, but in your case it may be another drive, depending on the number of drives connected to your workstation).
- **of** - stands for output file. Here, you should type the destination of your image in RAW format. In our case, it's `X:\ drive` and `147-2017.dd` file.
- **hash** - as has already been said, DC3DD supports four hashing algorithms: MD5, SHA-1, SHA-256, and SHA-512. We chose SHA-256, but you can choose whichever one you like.
- **log** - here, you should type the destination for the logs. You will find the image version, image hash, and so on in this file once acquisition is completed.

How it works...

DC3DD creates a bit-by-bit image of the source drive in RAW format, so the size of the image will be the same as the source, and it calculates the image hash using an algorithm of the examiner's choice, in our case SHA-256.

See also

The DC3DD download page:

`https://sourceforge.net/projects/dc3dd/files/dc3dd/7.2%20-%20Windows/`

Mounting forensic images with Arsenal Image Mounter

Arsenal Image Mounter is an open source tool developed by Arsenal Recon. It can help a digital forensic examiner to mount a forensic image or virtual machine disk in Windows. It supports both E01 (and EX01) and RAW forensic images, so you can use it with any of the images we created in the previous recipes.

It's very important to note that Arsenal Image Mounter mounts the contents of disk images as complete disks. The tool supports all file systems you can find on Windows drives: NTFS, ReFS, FAT32, and exFAT. Also, it has temporary write support for images, which is a very useful feature, for example, if you want to boot the system from the image you are examining.

Getting ready

Go to the Arsenal Image Mounter web page on the Arsenal Recon website and click on the download button to download the ZIP archive. At the time of writing, the latest version of the tool is 2.0.010, so in our case, the archive has the name **Arsenal_Image_Mounter_v2.0.010.0_x64.zip**. Extract it to a location of your choice and you are ready to go, no installation is required.

How to do it...

There two ways to choose an image for mounting in Arsenal Image Mounter.

- You can use the **File** menu (and choose **Mount image...**) or
- The **Mount image** button, as shown in figure 3.10

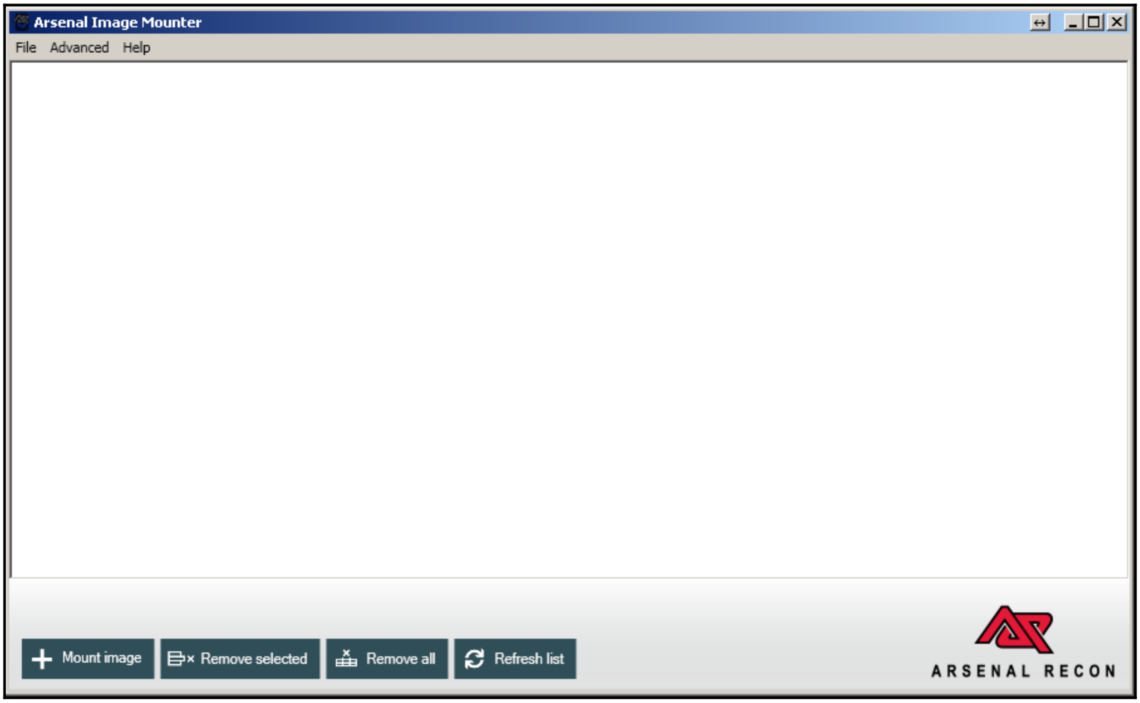
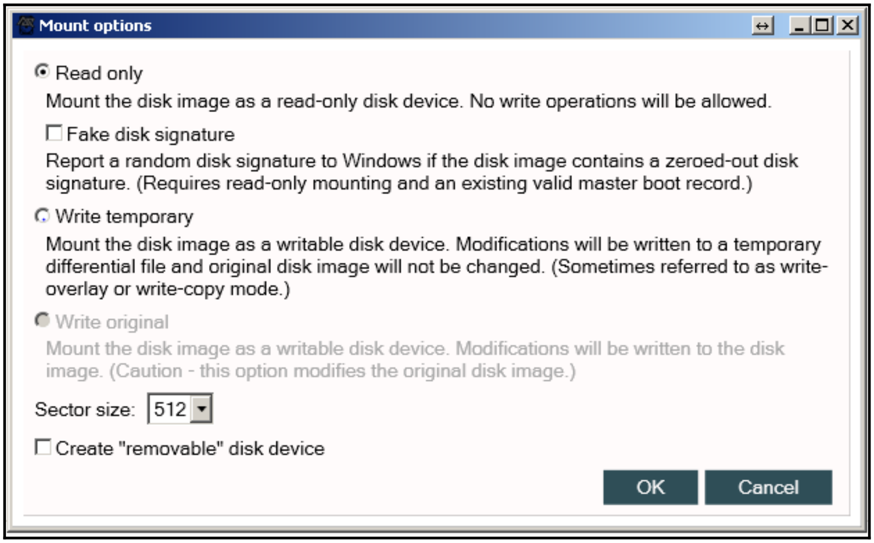


Figure 3.10. Arsenal Image Mounter main window

1. When you choose the **Mount image...** option from the **File** menu or click on the **Mount image** button, the **Open** window will pop up - here you should choose an image for mounting.

2. The next window you will see is **Mount options**, like the one in figure 3.11.



● Read only

Mount the disk image as a read-only disk device. No write operations will be allowed.

□ Fake disk signature

Report a random disk signature to Windows if the disk image contains a zeroed-out disk signature. (Requires read-only mounting and an existing valid master boot record.)

○ Write temporary

Mount the disk image as a writable disk device. Modifications will be written to a temporary differential file and original disk image will not be changed. (Sometimes referred to as write-overlay or write-copy mode.)

○ Write original

Mount the disk image as a writable disk device. Modifications will be written to the disk image. (Caution - this option modifies the original disk image.)

Sector size: 512

□ Create "removable" disk device

Figure 3.11. *Arsenal Image Mounter Mount options window*

As you can see, there are a few options here:

- **Read only** - if you choose this option, the image is mounted in read-only mode, so no write operations are allowed. (Do you still remember that you mustn't alter the evidence in any way? Of course, it's already an image, not the original drive, but nevertheless.)
- **Fake disk signature** - if an all-zero disk signature is found on the image, Arsenal Image Mounter reports a random disk signature to Windows, so it's mounted properly.
- **Write temporary** - if you choose this option, the image is mounted in read-write mode, but all modifications are written not in the original image file, but to a temporary differential file instead.
- **Write original** - again, this option mounts the image in read-write mode, but this time the original image file will be modified.
- **Sector size** - this option allows you to choose the sector size.
- **Create "removable" disk device** - this option emulates the attachment of a USB thumb drive.

3. Choose the options you think you need and click **OK**.

We decided to mount our image as **Read Only**. Now you can see a hard drive icon on the main window of the tool - the image is mounted.

If you mounted only one image and want to unmount it, select the image and click on **Remove selected**. If you have a few mounted images and want to unmount all of them, click on the **Remove all** button.

How it works...

Arsenal Image Mounter mounts forensic images or virtual machine disks as complete disks in read-only or read-write mode. Later, a digital forensics examiner can access their contents even with Windows Explorer.

See also

The Arsenal Image Mounter page on the Arsenal Recon website: `https://arsenalrecon.com/apps/image-mounter/`

4
Windows File System Analysis

In this chapter, we will cover the following recipes:

- NTFS analysis with The Sleuth Kit
- Undeleting files from NTFS with Autopsy
- Undeleting files from ReFS with ReclaiMe File Recovery
- File carving with PhotoRec

Introduction

As mentioned in the introductory section, Windows machines run on NTFS (**New Technology File System**).

Using the tools that we will discuss in this chapter, you will be able to uncover information not only about the files, but also about the layout of the disk itself, including deleted files and unallocated space. This can be of the utmost importance in a forensic investigation, particularly in cases where a user may have tried to cover up their actions using anti-forensic methods.

Some tools allow you to undelete files as well, thus restoring them, in whole or in part, to how they looked before they were deleted. This does, of course, depend on the extent to which a file has been overwritten, however it can be a useful way to find out about things a suspect doesn't want you to see.

In cases where the metadata about the files has been deleted, file carving is employed as a method of trying to recover the data within the files. This requires several steps, most of which will be performed by your investigative tool set of choice. Generally, it will begin by working out what type of file the item was (usually by looking at the headers), and then building up fragments of the file to form a more accurate picture of what used to be stored on the machine.

There are several solutions which deal with file system analysis, file carving, and the undeleting of files. In this chapter, we will be looking specifically at Autopsy, The Sleuth Kit, ReclaiMe, and PhotoRec.

NTFS Analysis with The Sleuth Kit

The Sleuth Kit is a collection of command-line tools (and also a library) for the forensic analysis of drive images. These tools can help you with analysis of both volume and file system data (in a non-intrusive fashion, of course). It's cross-platform, so you can use any operating system you like to work with this toolkit. It supports both RAW and E01 images, so you can use any image that you acquired while following the previous recipes. This collection of tools will be very useful in your future digital forensic examinations: it supports a wide range of file systems, including NTFS, FAT, ExFAT, EXT2, EXT3, EXT4, HFS, and so on.

Getting ready

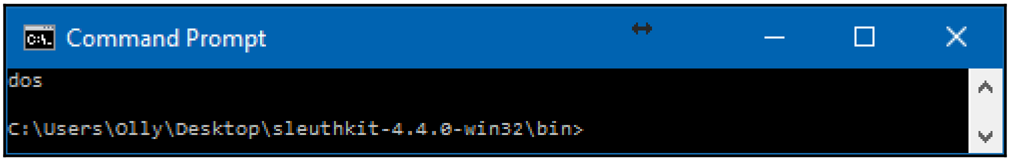
You can download Windows binaries from The Sleuth Kit's official website. Go to **The Sleuth Kit** section and click on the **Download** hyperlink. Now, click on **Windows Binaries** and the downloading will start. At the time of writing, the most recent version of The Sleuth Kit is 4.4.0, so the archive we downloaded has the name: **sleuthkit-4.4.0.tar.gz**. So, now all you need to do is to unpack it and you are ready to go.

How to do it...

Open Windows Command Prompt and change the directory to **bin** (you can find it in the folder where you unpacked the archive you downloaded). Let's start from the Media Management Layer Tools:

1. The first thing you should do is to figure out which system volume type you have. Of course, there is a tool for this in The Sleuth Kit. It's called `mmstat`. Let's use it on one of the images we acquired in the previous recipes:

```
mmstat X:146-2017.E01
```



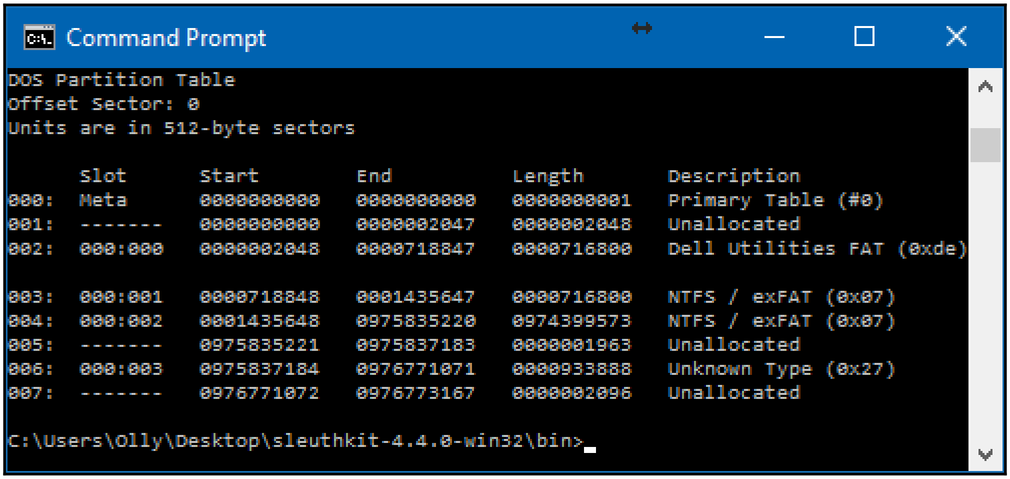
```
dos

C:\Users\Olly\Desktop\sleuthkit-4.4.0-win32\bin>
```

Figure 4.1. mmstat output

2. We now know the system volume type and are ready to use the next tool – `mmls`. This tool can help an examiner to determine the layout of a disk, including the unallocated space. Let's use it:

```
mmls -t dos X:146-2017.E01
```

The output of the preceding command is as follows:



```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000718847   0000716800   Dell Utilities FAT (0xde)

003:  000:001   0000718848   0001435647   0000716800   NTFS / exFAT (0x07)
004:  000:002   0001435648   0975835220   0974399573   NTFS / exFAT (0x07)
005:  -------   0975835221   0975837183   0000001963   Unallocated
006:  000:003   0975837184   0976771071   0000933888   Unknown Type (0x27)
007:  -------   0976771072   0976773167   0000002096   Unallocated

C:\Users\Olly\Desktop\sleuthkit-4.4.0-win32\bin>
```

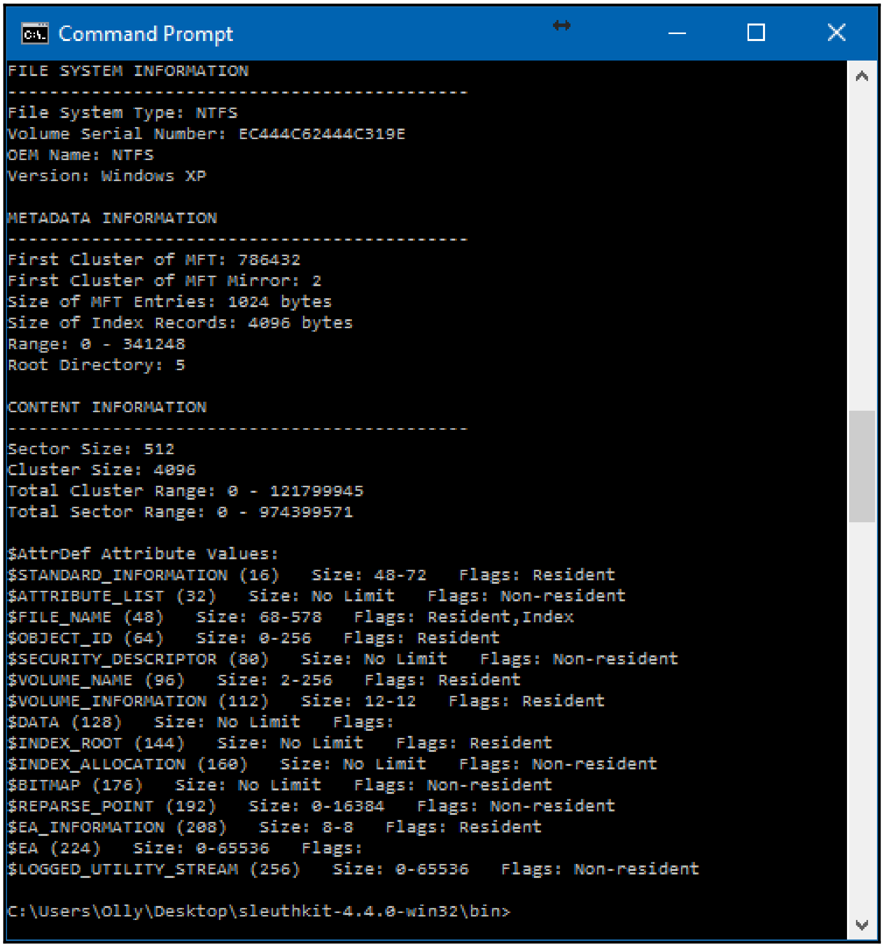
Figure 4.2. mmls output

As you can see, we have gathered a lot of valuable information about our disk (as you remember, we imaged a drive in the previous recipes). Now you know the starting sectors, ending sectors, and lengths of all partitions and unallocated spaces.

3. Let's change to File System Layer Tools. To learn more about each of the partitions, we have the `fsstat` tool. To use it, we need the partition offset. You can get it from the `mmls` output. Let's learn more about the largest partition we have, which starts at sector 1435658:

```
fsstat -o 1435648 X:146-2017.E01
```

The output of the preceding command is as follows:



```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: EC444C62444C319E
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 341248
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 121799945
Total Sector Range: 0 - 974399571

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident

C:\Users\Olly\Desktop\sleuthkit-4.4.0-win32\bin>
```

Figure 4.3. fsstat output

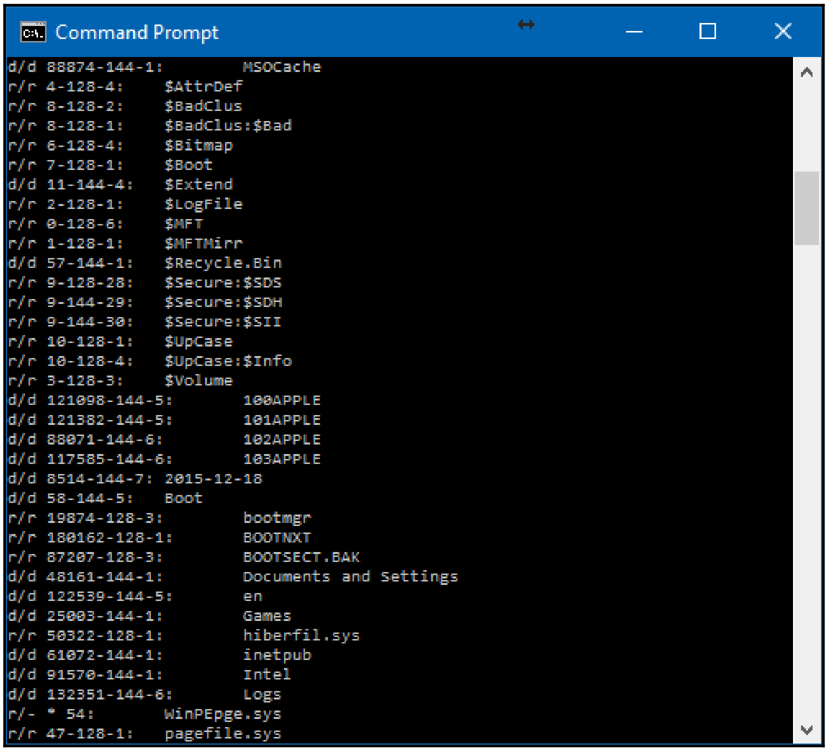
As you can see in the preceding figure, `fsstat` collects lots of useful information about a partition: **Volume Serial Number**, **Cluster Size**, **First Cluster of MFT**, **First Cluster of MFT mirror,** and so on.

> The MFT, or Master File Table, contains information about all files, directories, and metafiles in NTFS, including their names, creation timestamps, sizes, and access permissions.

4. Let's now look at FileName Layer Tools. For example, the `fls` tool allows examiners to list allocated and deleted file names in a directory. Again, we need the partition offset to use this tool:

```
fls -o 1435648 X:146-2017.E01
```

The output for the preceding command is as follows:



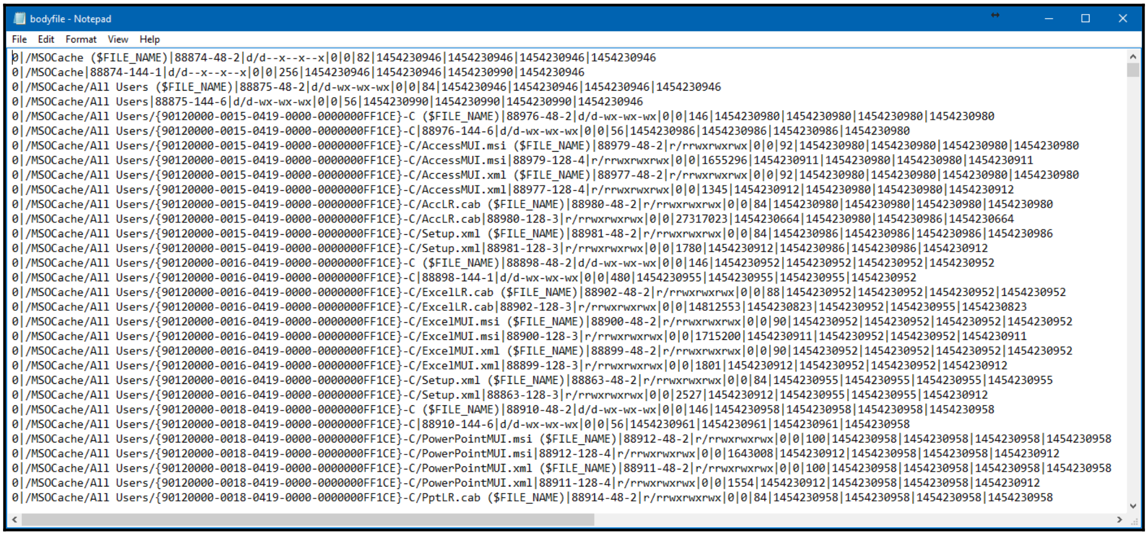
```
d/d 88874-144-1:        MSOCache
r/r 4-128-4:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
d/d 57-144-1:   $Recycle.Bin
r/r 9-128-28:   $Secure:$SDS
r/r 9-144-29:   $Secure:$SDH
r/r 9-144-30:   $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
d/d 121098-144-5:       100APPLE
d/d 121382-144-5:       101APPLE
d/d 88071-144-6:        102APPLE
d/d 117585-144-6:       103APPLE
d/d 8514-144-7: 2015-12-18
d/d 58-144-5:   Boot
r/r 19874-128-3:        bootmgr
r/r 180162-128-1:       BOOTNXT
r/r 87207-128-3:        BOOTSECT.BAK
d/d 48161-144-1:        Documents and Settings
d/d 122539-144-5:       en
d/d 25003-144-1:        Games
r/r 50322-128-1:        hiberfil.sys
d/d 61072-144-1:        inetpub
d/d 91570-144-1:        Intel
d/d 132351-144-6:       Logs
r/- * 54:       WinPEpge.sys
r/r 47-128-1:   pagefile.sys
```

Figure 4.4. A part of fls output

5. Let's go further and create a `bodyfile` with `fls`. It's truly an amazing feature that helps Windows forensic examiners to create timelines of file activity. Here is how we create it:

   ```
   fls -r -m "/" -o 1435648 X:146-2017.E01 > bodyfile.txt
   ```

   The output for the preceding command is as follows:



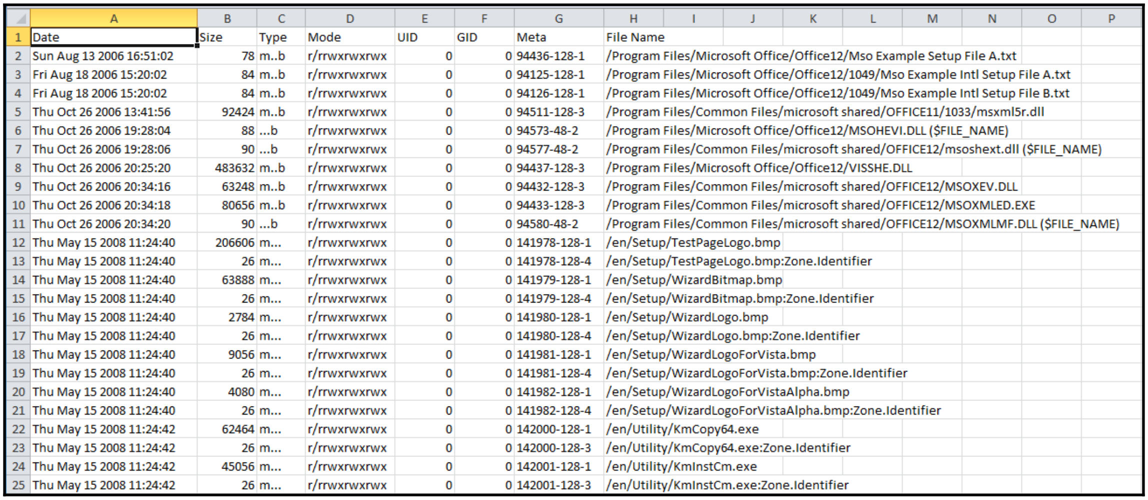
```
0|/MSOCache ($FILE_NAME)|88874-48-2|d/d--x--x--x|0|0|82|1454230946|1454230946|1454230946|1454230946
0|/MSOCache|88874-144-1|d/d--x--x--x|0|0|256|1454230946|1454230946|1454230990|1454230946
0|/MSOCache/All Users ($FILE_NAME)|88875-48-2|d/d-wx-wx-wx|0|0|84|1454230946|1454230946|1454230946|1454230946
0|/MSOCache/All Users|88875-144-6|d/d-wx-wx-wx|0|0|56|1454230990|1454230990|1454230990|1454230946
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C ($FILE_NAME)|88976-48-2|d/d-wx-wx-wx|0|0|146|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C|88976-144-6|d/d-wx-wx-wx|0|0|56|1454230986|1454230986|1454230986|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.msi ($FILE_NAME)|88979-48-2|r/rrwxrwxrwx|0|0|92|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.msi|88979-128-4|r/rrwxrwxrwx|0|0|1655296|1454230911|1454230980|1454230980|1454230911
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.xml ($FILE_NAME)|88977-48-2|r/rrwxrwxrwx|0|0|92|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccessMUI.xml|88977-128-4|r/rrwxrwxrwx|0|0|1345|1454230912|1454230980|1454230980|1454230912
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccLR.cab ($FILE_NAME)|88980-48-2|r/rrwxrwxrwx|0|0|84|1454230980|1454230980|1454230980|1454230980
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/AccLR.cab|88980-128-3|r/rrwxrwxrwx|0|0|27317023|1454230664|1454230980|1454230986|1454230664
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/Setup.xml ($FILE_NAME)|88981-48-2|r/rrwxrwxrwx|0|0|84|1454230986|1454230986|1454230986|1454230986
0|/MSOCache/All Users/{90120000-0015-0419-0000-0000000FF1CE}-C/Setup.xml|88981-128-3|r/rrwxrwxrwx|0|0|1780|1454230912|1454230986|1454230986|1454230912
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C ($FILE_NAME)|88898-48-2|d/d-wx-wx-wx|0|0|146|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C|88898-144-1|d/d-wx-wx-wx|0|0|480|1454230955|1454230955|1454230955|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelLR.cab ($FILE_NAME)|88902-48-2|r/rrwxrwxrwx|0|0|88|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelLR.cab|88902-128-3|r/rrwxrwxrwx|0|0|14812553|1454230823|1454230952|1454230955|1454230823
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.msi ($FILE_NAME)|88900-48-2|r/rrwxrwxrwx|0|0|90|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.msi|88900-128-3|r/rrwxrwxrwx|0|0|1715200|1454230911|1454230952|1454230952|1454230911
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.xml ($FILE_NAME)|88899-48-2|r/rrwxrwxrwx|0|0|90|1454230952|1454230952|1454230952|1454230952
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/ExcelMUI.xml|88899-128-3|r/rrwxrwxrwx|0|0|1801|1454230912|1454230952|1454230952|1454230912
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/Setup.xml ($FILE_NAME)|88863-48-2|r/rrwxrwxrwx|0|0|84|1454230955|1454230955|1454230955|1454230955
0|/MSOCache/All Users/{90120000-0016-0419-0000-0000000FF1CE}-C/Setup.xml|88863-128-3|r/rrwxrwxrwx|0|0|2527|1454230912|1454230955|1454230955|1454230912
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C ($FILE_NAME)|88910-48-2|d/d-wx-wx-wx|0|0|146|1454230958|1454230958|1454230958|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C|88910-144-6|d/d-wx-wx-wx|0|0|56|1454230961|1454230961|1454230961|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.msi ($FILE_NAME)|88912-48-2|r/rrwxrwxrwx|0|0|100|1454230958|1454230958|1454230958|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.msi|88912-128-4|r/rrwxrwxrwx|0|0|1643008|1454230912|1454230958|1454230958|1454230912
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.xml ($FILE_NAME)|88911-48-2|r/rrwxrwxrwx|0|0|100|1454230958|1454230958|1454230958|1454230958
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PowerPointMUI.xml|88911-128-4|r/rrwxrwxrwx|0|0|1554|1454230912|1454230958|1454230958|1454230912
0|/MSOCache/All Users/{90120000-0018-0419-0000-0000000FF1CE}-C/PptLR.cab ($FILE_NAME)|88914-48-2|r/rrwxrwxrwx|0|0|84|1454230958|1454230958|1454230958|1454230958
```

Figure 4.5. A part of bodyfile created with fls

   As you can see, we added two switches in the command: `-r` and `-m`. The first one tells `fls` to recurse the directory entries. The second tells it to use `mactime` input format with / as the mount point.

6. We now have the body file, so we are ready to run `mactime` and create a timeline of file activity. Such timelines are very useful in Windows forensic examinations, especially in cases involving malware incidents. Here is how to create it:

   ```
   mactime.pl -b bodyfile.txt -d > timeline.csv
   ```



	A	B	C	D	E	F	G	H
1	Date	Size	Type	Mode	UID	GID	Meta	File Name
2	Sun Aug 13 2006 16:51:02	78	m..b	r/rrwxrwxrwx	0	0	94436-128-1	/Program Files/Microsoft Office/Office12/Mso Example Setup File A.txt
3	Fri Aug 18 2006 15:20:02	84	m..b	r/rrwxrwxrwx	0	0	94125-128-1	/Program Files/Microsoft Office/Office12/1049/Mso Example Intl Setup File A.txt
4	Fri Aug 18 2006 15:20:02	84	m..b	r/rrwxrwxrwx	0	0	94126-128-1	/Program Files/Microsoft Office/Office12/1049/Mso Example Intl Setup File B.txt
5	Thu Oct 26 2006 13:41:56	92424	m..b	r/rrwxrwxrwx	0	0	94511-128-3	/Program Files/Common Files/microsoft shared/OFFICE11/1033/msxml5r.dll
6	Thu Oct 26 2006 19:28:04	88	...b	r/rrwxrwxrwx	0	0	94573-48-2	/Program Files/Microsoft Office/Office12/MSOHEVI.DLL ($FILE_NAME)
7	Thu Oct 26 2006 19:28:06	90	...b	r/rrwxrwxrwx	0	0	94577-48-2	/Program Files/Common Files/microsoft shared/OFFICE12/msoshext.dll ($FILE_NAME)
8	Thu Oct 26 2006 20:25:20	483632	m..b	r/rrwxrwxrwx	0	0	94437-128-3	/Program Files/Microsoft Office/Office12/VISSHE.DLL
9	Thu Oct 26 2006 20:34:16	63248	m..b	r/rrwxrwxrwx	0	0	94432-128-3	/Program Files/Common Files/microsoft shared/OFFICE12/MSOXEV.DLL
10	Thu Oct 26 2006 20:34:18	80656	m..b	r/rrwxrwxrwx	0	0	94433-128-3	/Program Files/Common Files/microsoft shared/OFFICE12/MSOXMLED.EXE
11	Thu Oct 26 2006 20:34:20	90	...b	r/rrwxrwxrwx	0	0	94580-48-2	/Program Files/Common Files/microsoft shared/OFFICE12/MSOXMLMF.DLL ($FILE_NAME)
12	Thu May 15 2008 11:24:40	206606	m...	r/rrwxrwxrwx	0	0	141978-128-1	/en/Setup/TestPageLogo.bmp
13	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141978-128-4	/en/Setup/TestPageLogo.bmp:Zone.Identifier
14	Thu May 15 2008 11:24:40	63888	m...	r/rrwxrwxrwx	0	0	141979-128-1	/en/Setup/WizardBitmap.bmp
15	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141979-128-4	/en/Setup/WizardBitmap.bmp:Zone.Identifier
16	Thu May 15 2008 11:24:40	2784	m...	r/rrwxrwxrwx	0	0	141980-128-1	/en/Setup/WizardLogo.bmp
17	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141980-128-4	/en/Setup/WizardLogo.bmp:Zone.Identifier
18	Thu May 15 2008 11:24:40	9056	m...	r/rrwxrwxrwx	0	0	141981-128-1	/en/Setup/WizardLogoForVista.bmp
19	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141981-128-4	/en/Setup/WizardLogoForVista.bmp:Zone.Identifier
20	Thu May 15 2008 11:24:40	4080	m...	r/rrwxrwxrwx	0	0	141982-128-1	/en/Setup/WizardLogoForVistaAlpha.bmp
21	Thu May 15 2008 11:24:40	26	m...	r/rrwxrwxrwx	0	0	141982-128-4	/en/Setup/WizardLogoForVistaAlpha.bmp:Zone.Identifier
22	Thu May 15 2008 11:24:42	62464	m...	r/rrwxrwxrwx	0	0	142000-128-1	/en/Utility/KmCopy64.exe
23	Thu May 15 2008 11:24:42	26	m...	r/rrwxrwxrwx	0	0	142000-128-3	/en/Utility/KmCopy64.exe:Zone.Identifier
24	Thu May 15 2008 11:24:42	45056	m...	r/rrwxrwxrwx	0	0	142001-128-1	/en/Utility/KmInstCm.exe
25	Thu May 15 2008 11:24:42	26	m...	r/rrwxrwxrwx	0	0	142001-128-3	/en/Utility/KmInstCm.exe:Zone.Identifier

Figure 4.6. The timeline file opened in Microsoft Excel

Again, in the last command we have two switches which need to be explained. The first one, `-b`, points to the bodyfile for `mactime` to use. The second, `-d`, stands for delimited output and means we can save it as a CSV file and use Microsoft Excel or OpenOffice Spreadsheets to work with it later (see the figure above). Also, if you want to specify the time zone, you can use the `-z` switch.

How it works...

Below is a list of the main commands used and their functions:

- `mmstat`: extracts information about the system volume type
- `mmls`: extracts information about disk layout, including unallocated spaces
- `fsstat`: extracts information about a file system, including volume serial number, cluster size, and so on
- `fls`: extracts information about both allocated and deleted file names in a directory
- `mactime`: creates a timeline of file activity based on a body file created with `fls`

See also

The Sleuth Kit download page: `https://www.sleuthkit.org/sleuthkit/download.php`

The Sleuth Kit wiki: `http://wiki.sleuthkit.org/index.php?title=Main_Page`

Undeleting files from NTFS with Autopsy

Originally, **Autopsy** was just a graphical interface for The Sleuth Kit. You have already learnt about the collection of command-line tools for file system forensic analysis in the previous recipe. Since the third version however, it has been totally rewritten and is now available as a standalone digital forensics platform. It is very widely used and forms part of the digital forensic toolkit of both law enforcement and corporate examiners. Why? It's easy to use, fast, and free. Also, if you enjoy programming, you can write your own modules for Autopsy - all the documentation you will need is freely available online, on The Sleuth Kit's website. Basis Technology even holds Autopsy module writing contests, so feel free to participate.

Getting ready...

Go to The Sleuth Kit's website again, but now choose **Autopsy,** and after that, **Download**. The most recent version at the time of writing is 4.3.0. Both 32- and 64-bit versions are available; you should choose the right one according to your system (we have already shown you how to collect this piece of information in one of the previous recipes). You will be redirected to SourceForge, and the downloading process will start automatically. In our case, the file we downloaded is named **autopsy-4.3.0-64bit.msi.** All you need now is to double-click it and follow the installation instructions, which are quite straightforward. Once the installation process is complete, you are ready to go.

How to do it...

After starting your freshly installed digital forensics tool, the first window you see is **Welcome**. Here we have three main options:

- **Create New Case** - this option will create a new case for you
- **Open Recent Case** - this option will open the last case you worked on
- **Open Existing Case** - this option allows you to choose one of the cases present on your workstation

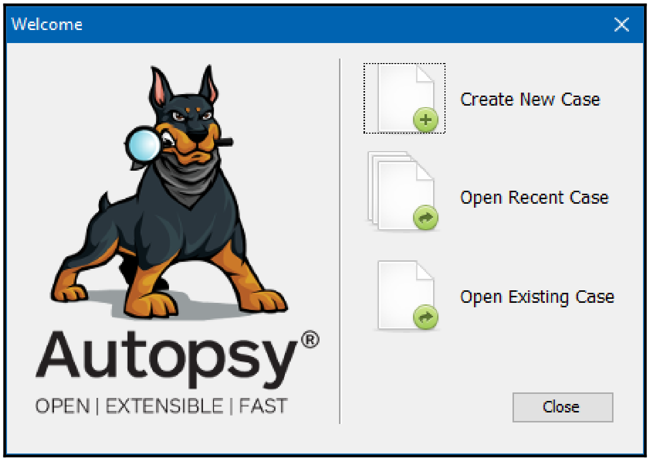
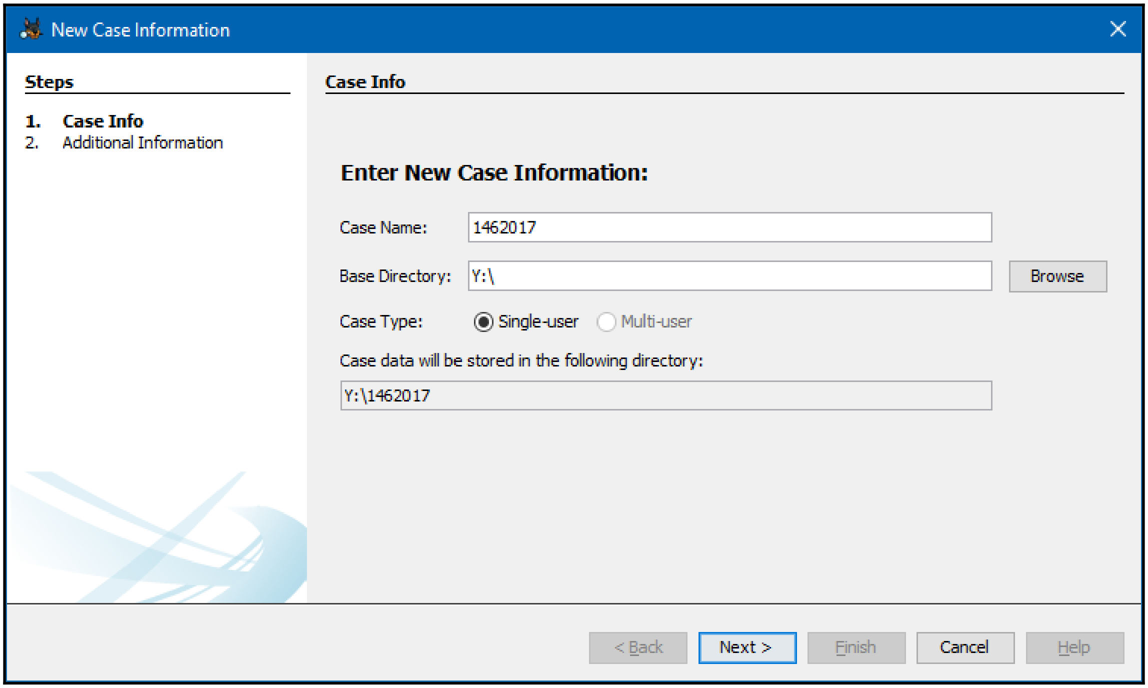


Figure 4.7. Autopsy Welcome window

As we just installed Autopsy, we don't have any cases, so our choice is the **Create New Case** option. Now you will see a **New Case Information** window.

1. In the first step, **Case Info**, we have two fields to fill in; the third will be completed automatically. You should type your case number or name in the first field, **Case Name**, and choose the directory for your case files in the second, **Base Directory** (use the **Browse** button). The third field will show the path to your case files (base directory + case name).



Enter New Case Information:

Case Name: 1462017

Base Directory: Y:\

Browse

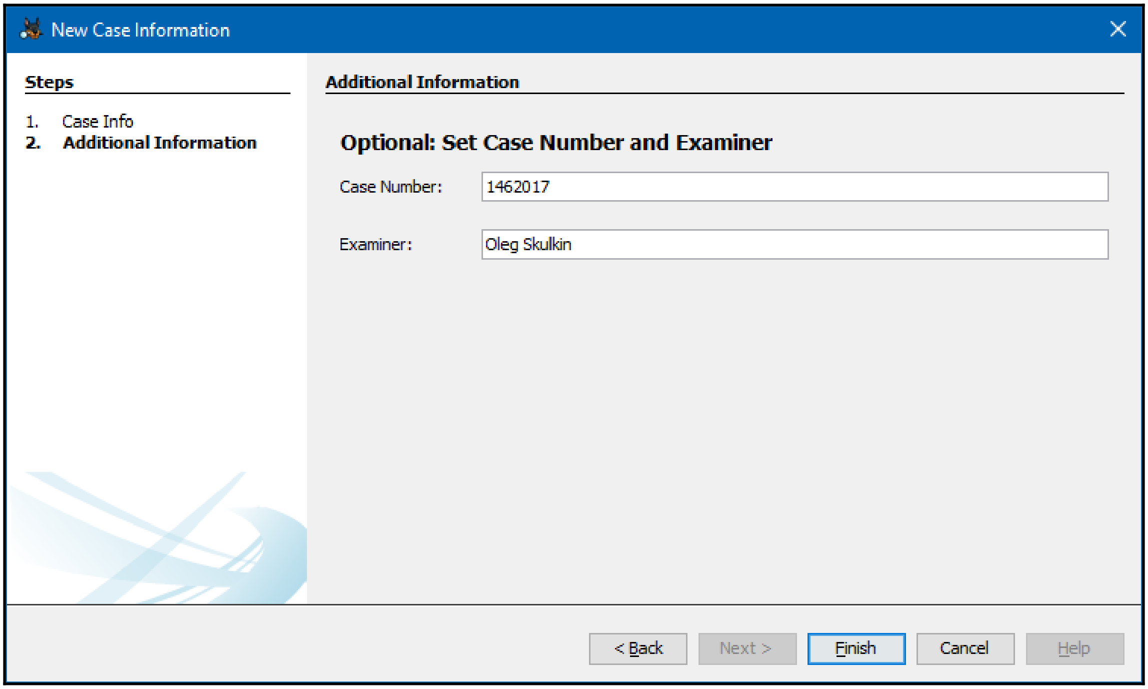
Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

Y:\1462017

Figure 4.8. Autopsy New Case Information (Case Info) window

2. The second step, **Additional Information**, is optional: you can leave both fields blank. However, it is usually better to fill them in. The first field should contain your case number, the second your name.



New Case Information

Steps

1. Case Info
2. **Additional Information**

Additional Information

Optional: Set Case Number and Examiner

Case Number: 1462017

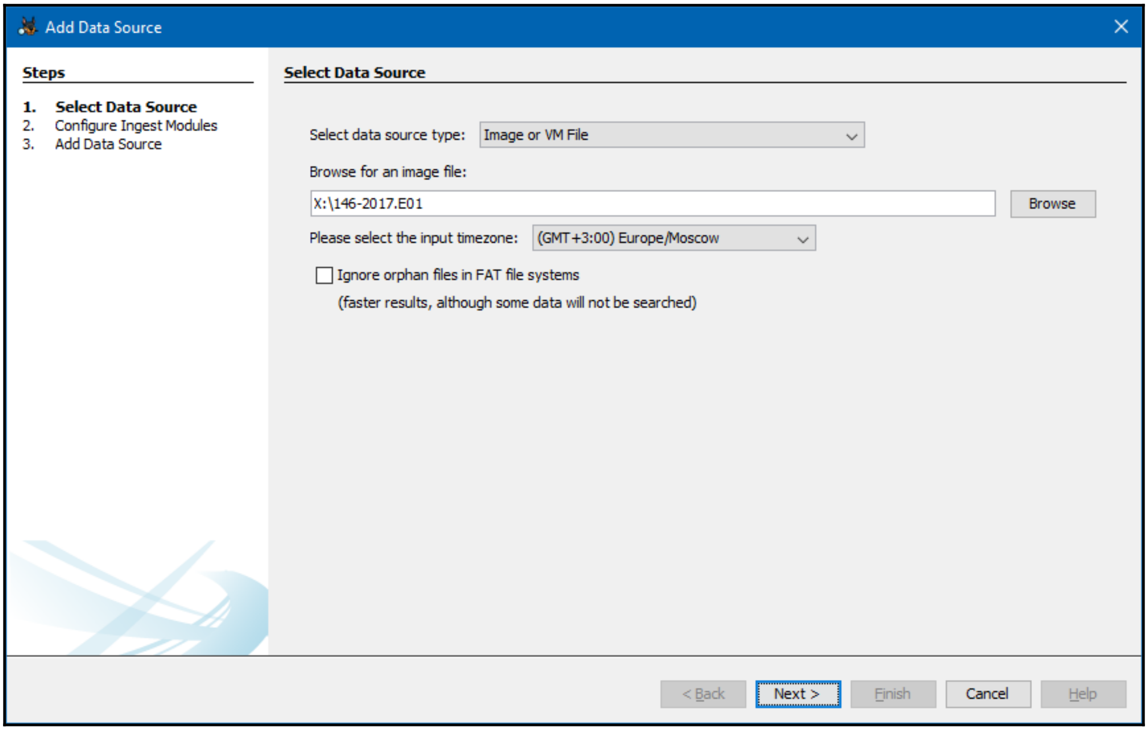
Examiner: Oleg Skulkin

Figure 4.9. Autopsy New Case Information (Additional Information) window

3. Click **Finish** and the case will be created.
4. It's time to select the data source, here is the **Add Data Source** window. The first thing you should do is select the data source type. Three options are available:

   - **Image or VM File** - this option allows you to choose a forensic image in one of the supported formats, or a virtual machine disk, for example, that was found during the examination of an image
   - **Local Disk** - this option allows you to choose a physical drive connected to your workstation, or a mounted logical drive (for example, D:)

- **Logical Files** - this option allows you to choose files and folders for analysis, for example, from a mounted forensic image



Add Data Source

Steps

1. **Select Data Source**
2. Configure Ingest Modules
3. Add Data Source

Select Data Source

Select data source type: Image or VM File

Browse for an image file:

X:\146-2017.E01

Please select the input timezone: (GMT+3:00) Europe/Moscow

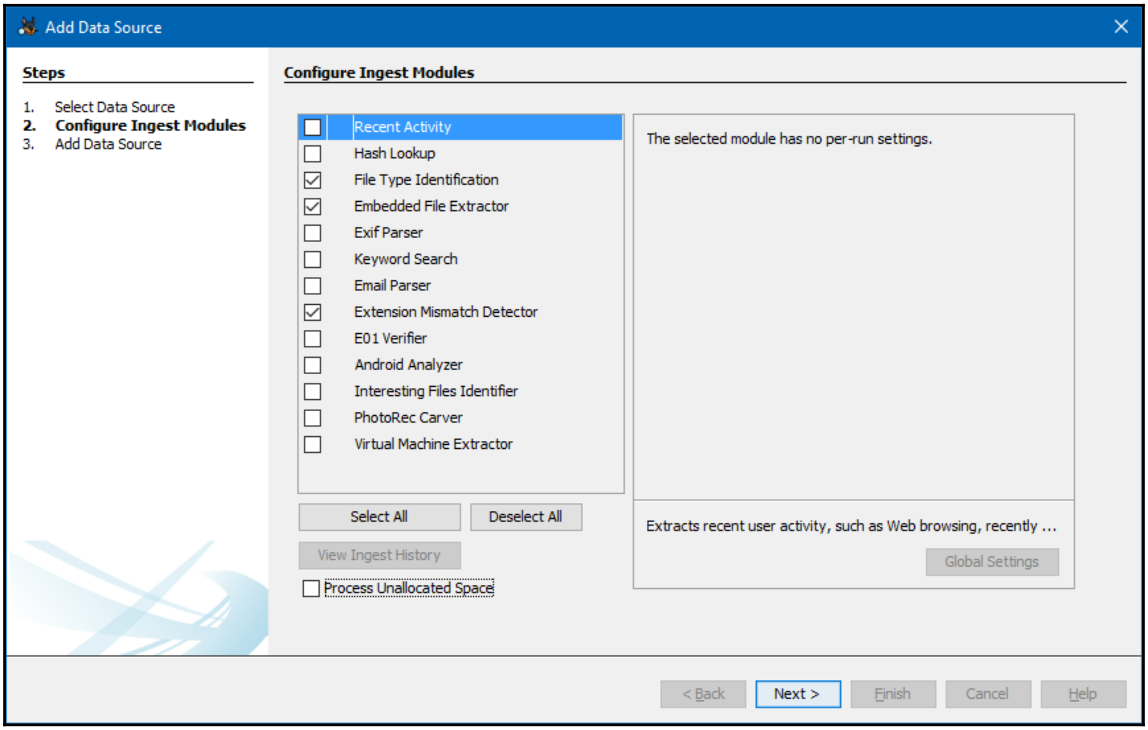
□ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

Figure 4.10. Autopsy Select Data Source window

5. Don't forget to choose the right time zone.
6. In the next step, you should choose ingest modules to run. Autopsy ingest modules analyze the files on the data source and parse their contents. As the main aim of this recipe is to show you how to undelete files from NTFS, we have chosen just a few modules, including:

   - **File type identification** - identifies files based not on their extensions, but their internal signatures
   - **Extension mismatch detector** - uses File Type Identification Module results to flag the files with an extension that is not usually associated with the detected file type

- **Embedded file extractor** - extracts data from different archive formats, including DOCX, XLSX, PPTX, and others



Add Data Source

Steps

1. Select Data Source
2. **Configure Ingest Modules**
3. Add Data Source

Configure Ingest Modules

☐ Recent Activity
☐ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☐ Exif Parser
☐ Keyword Search
☐ Email Parser
☑ Extension Mismatch Detector
☐ E01 Verifier
☐ Android Analyzer
☐ Interesting Files Identifier
☐ PhotoRec Carver
☐ Virtual Machine Extractor

☐ Process Unallocated Space

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently ...

Figure 4.11. Autopsy Select Data Source (Configure Ingest Modules) window

7. Click **Next** and data source processing will start.
8. After some time, depending on the size of the data source, the **Finish** button will become active: click it and you are ready to analyze the file system(s).

The point of this recipe is to teach you how to undelete files from NTFS. The thing is, when a file is deleted, it's not erased; it is simply marked as deleted in the MFT entry for the file. So, until the file is overwritten, it can be recovered, and Autopsy can help digital forensic examiners with this. It even sorts out all the deleted files for you: just go to **Views - Deleted Files** on the left pane (the Tree Viewer).

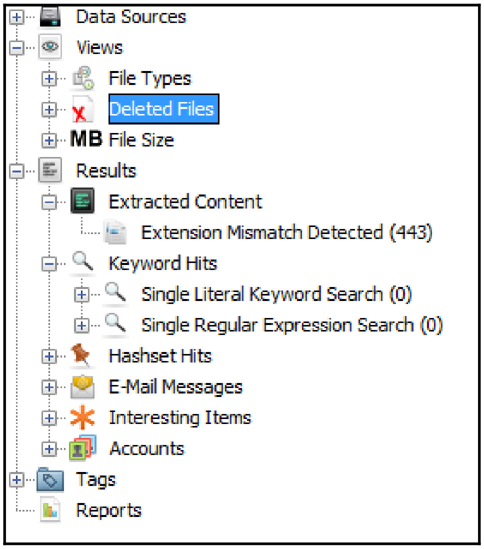


Figure 4.12. Deleted Files option in the Tree Viewer

You can use this option to recover files, or browse the file system(s) via the **Data Sources** option. Deleted files have red cross icons on the left. To recover a file or files:

1. Right-click on the file or files (mark all the files you want to recover beforehand)
2. Choose **Extract File(s)**
3. Choose the destination folder
4. Click **Save**

Yes, it is that easy!

How it works...

Autopsy detects files marked as deleted in the MFT and sorts them all out, so a digital forensic examiner can locate such files and recover them.

See also

Autopsy download page: `http://sleuthkit.org/autopsy/download.php`

Autopsy User's Guide: `http://sleuthkit.org/autopsy/docs/user-docs/3.1/index.html`

Undeleting files from ReFS with ReclaiMe File Recovery

ReclaiMe File Recovery is a piece of data recovery software capable of undeleting files from a wide range of devices including hard drives, memory cards, RAID arrays, and multi-disk NAS devices. Also, it supports data recovery from most file systems, including the latest Windows file systems - **ReFS** or the **Resilient File System**.

Getting ready

Go to ReClaiMe's website and click on the green **DOWNLOAD** button on the left. It brings you to the ReclaiMe File Recovery download page and the downloading process starts automatically. After this, just run the setup file and follow the installation instructions. You are ready to go!

How to do it...

Before you start, it's a good idea to find the right data source. ReFS is an active development, and is used usually on Windows servers only. Thankfully, Willi Ballenthin has created a bunch of ReFS images for testing purposes, which are now publically available. Let's use one of them.

1. Start ReclaiMe File Recovery. It takes some time for the tool to scan all available drives. After this, you will be taken to the main window, like the one in the following figure:

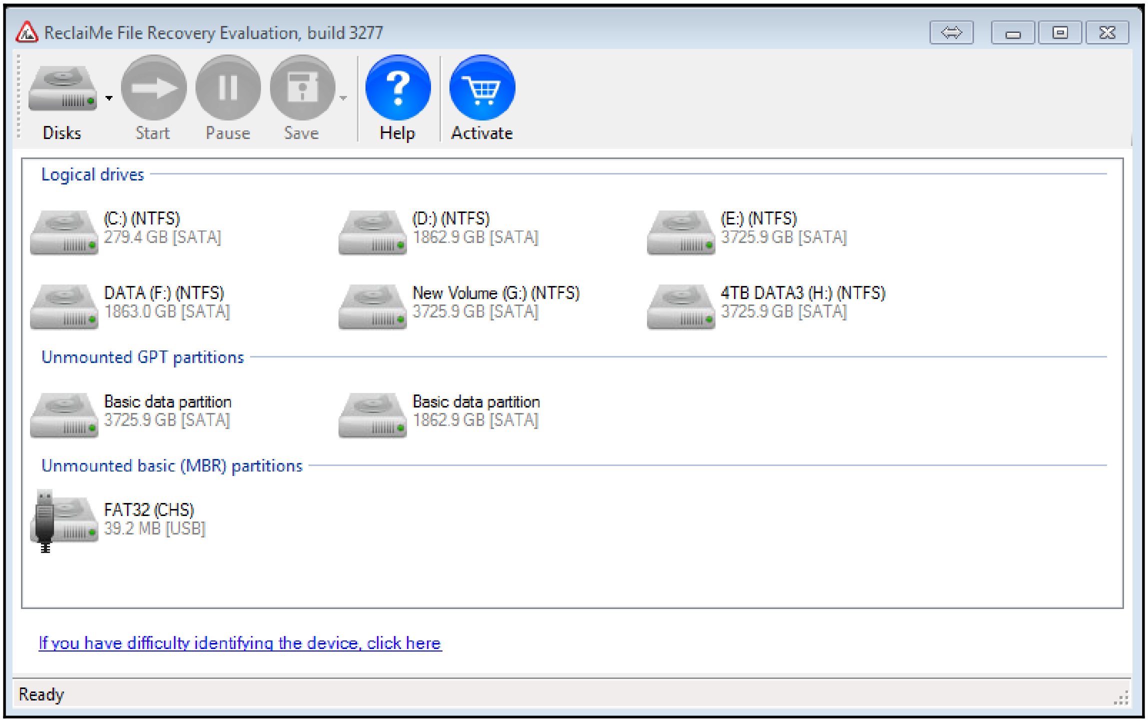
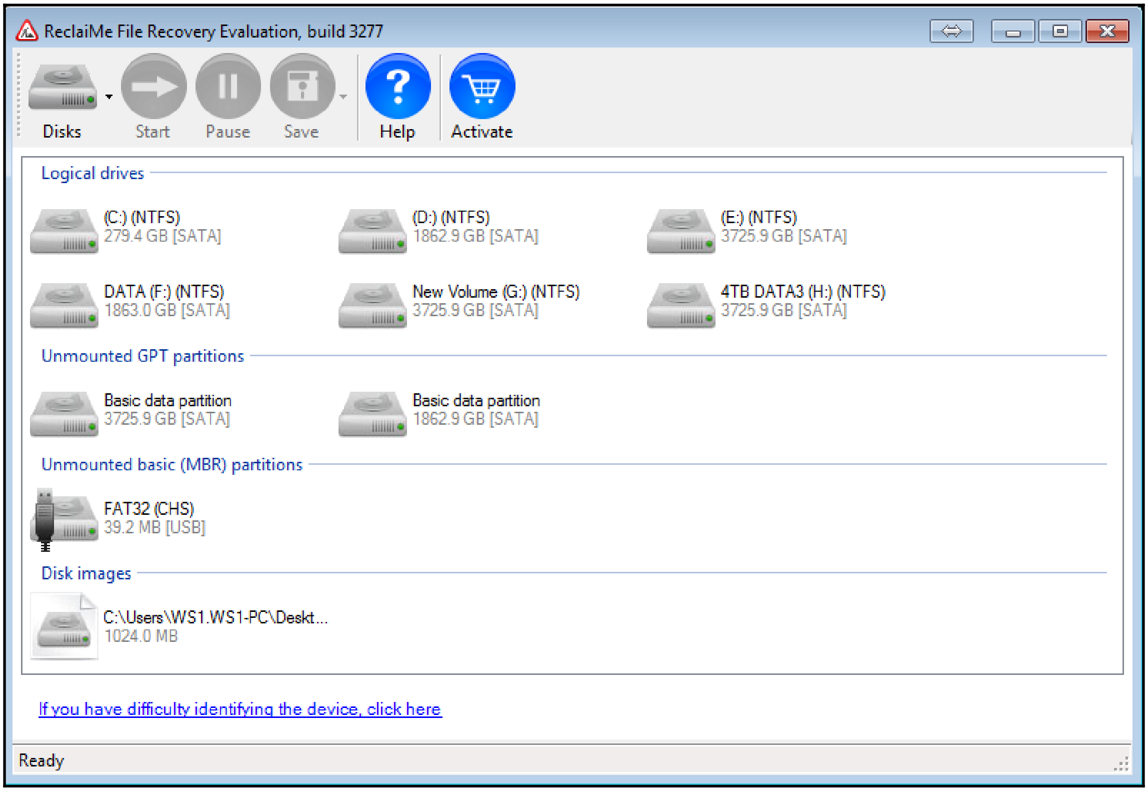


Figure 4.13. ReclaiMe File Recovery main window

ReclaiMe File Recovery doesn't support E01 images, but this is not a problem because we have an image in RAW format.

2. Let's go to **Disks - Open disk image...** Choose the disk image and click Open. Now there should also be an image in the main window, like the one in the following figure:



Logical drives

(C:) (NTFS)
279.4 GB [SATA]

(D:) (NTFS)
1862.9 GB [SATA]

(E:) (NTFS)
3725.9 GB [SATA]

DATA (F:) (NTFS)
1863.0 GB [SATA]

New Volume (G:) (NTFS)
3725.9 GB [SATA]

4TB DATA3 (H:) (NTFS)
3725.9 GB [SATA]

Unmounted GPT partitions

Basic data partition
3725.9 GB [SATA]

Basic data partition
1862.9 GB [SATA]

Unmounted basic (MBR) partitions

FAT32 (CHS)
39.2 MB [USB]

Disk images

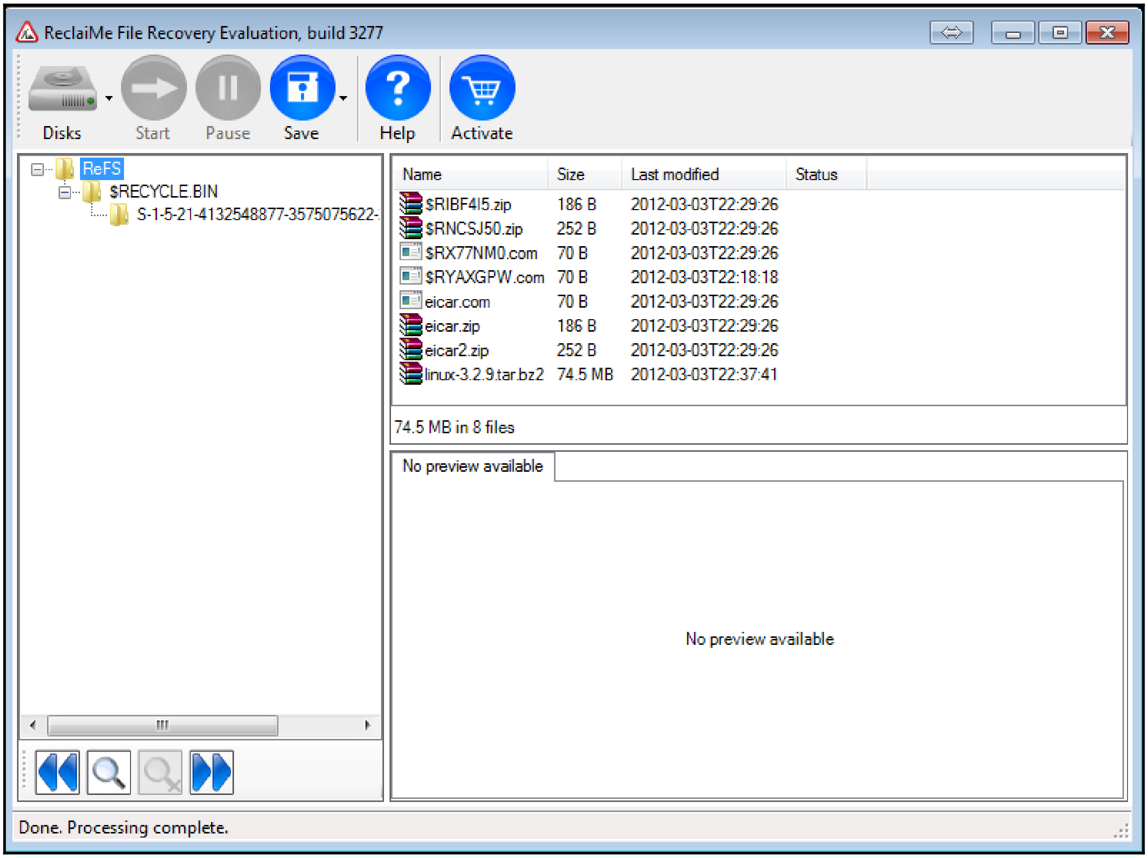
C:\Users\WS1.WS1-PC\Deskt...
1024.0 MB

If you have difficulty identifying the device, click here

Ready

Figure 4.14. ReclaiMe File Recovery main window (Disk image is added)

3. Double-click the image to start the recovery process. Of course, it will take some time, depending on the size of the image. In our case, the image is small enough, so it doesn't take a lot of time. The recovery is shown in the following figure:


ReclaiMe File Recovery Evaluation, build 3277
Disks
Start
Pause
Save
Help
Activate
ReFS
$RECYCLE.BIN
S-1-5-21-4132548877-3575075622-

Name	Size	Last modified	Status
$RIBF4I5.zip	186 B	2012-03-03T22:29:26	
$RNCSJ50.zip	252 B	2012-03-03T22:29:26	
$RX77NM0.com	70 B	2012-03-03T22:29:26	
$RYAXGPW.com	70 B	2012-03-03T22:18:18	
eicar.com	70 B	2012-03-03T22:29:26	
eicar.zip	186 B	2012-03-03T22:29:26	
eicar2.zip	252 B	2012-03-03T22:29:26	
linux-3.2.9.tar.bz2	74.5 MB	2012-03-03T22:37:41	

74.5 MB in 8 files

No preview available

No preview available

Done. Processing complete.

Figure 4.15. ReclaiMe File Recovery image processing results

4. Now you can save recovered files or even folders using the blue **Save** button.

How it works...

ReclaiMe File Recovery processes the image and lists the files and folders available, giving a computer forensic examiner the ability to extract deleted files.

See also

The ReclaiMe File Recovery website: `http://www.reclaime.com/`

The ReFS sample images: `http://www.williballenthin.com/forensics/refs/test_images/`

File carving with PhotoRec

PhotoRec is a file carving tool that is widely used by digital forensic examiners. This tool is even built into the previously mentioned digital forensic platform, Autopsy, as a module. PhotoRec can recover a diverse range of file types (more than 480 file formats), but if you think this will not be enough, you can add your own custom signatures, which will help the tool to recover even more data.

Getting ready

Go to CGSecurity's website and click the **download** hyperlink on the left. You will be redirected to the Download page. Now click on the big green button on the right, and the downloading process will be initiated. At the time of writing, the most recent version of PhotoRec is 7.0, so the archive we downloaded is called **testdisk-7.0.win.zip**. Unpack it and you are ready to go.

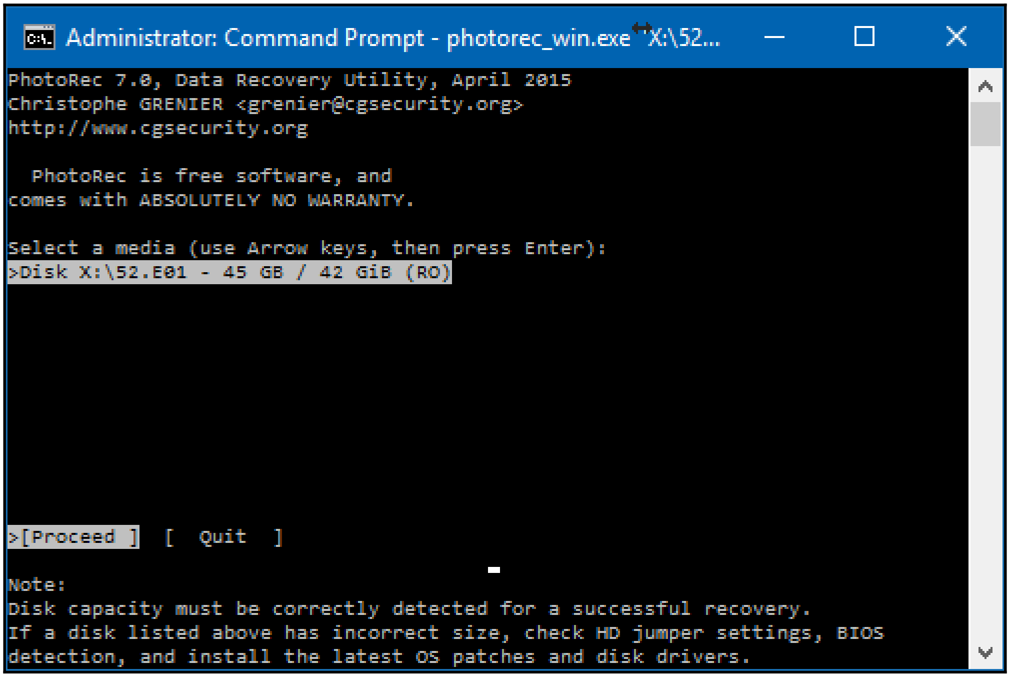
How to do it...

Before we start, it's important to note that PhotoRec supports disk images: not only RAW, but also E01. As we are carving data for forensic purposes, let's use an E01 image that we acquired in one of the previous recipes.

1. Start the Windows Command Prompt from an account in the Administrator group, and change the directory to **testdisk-7.0**. Use the following command:

   ```
   photorec_win.exe X:52.E01
   ```

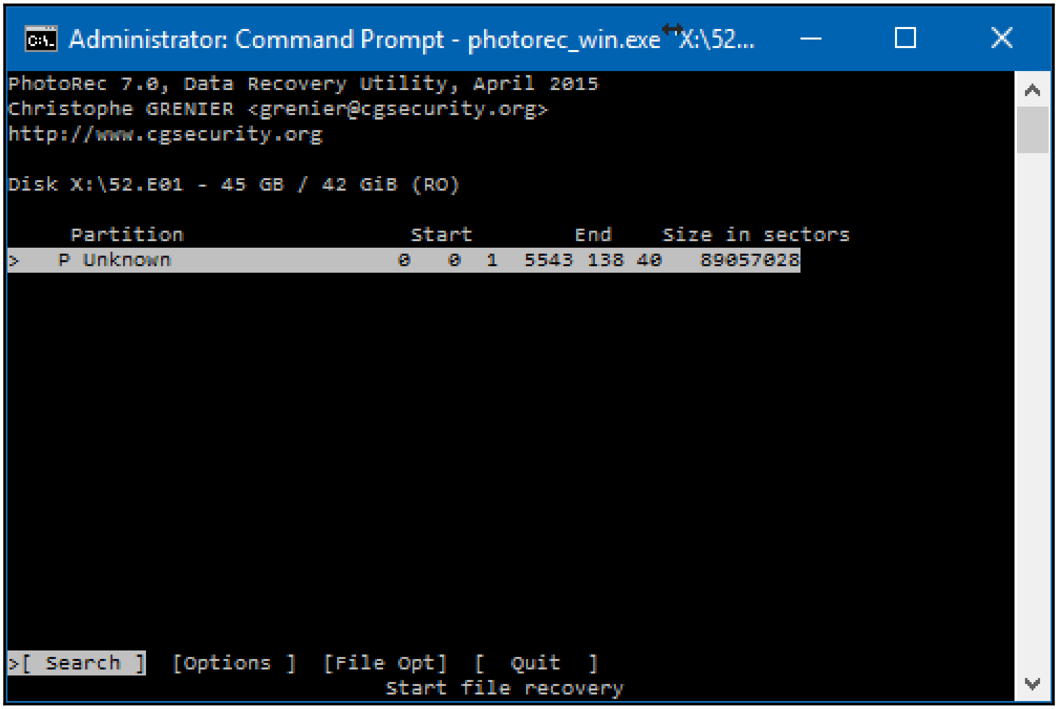
2. Make sure you typed the path to the image you acquired, as it can have a different name and location.
3. The first dialog box that you see is 'Select a media'. In our case we are dealing with an E01 image, so we have only one option, and all we need to do is press *Enter* to proceed.



```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk X:\52.E01 - 45 GB / 42 GiB (RO)









>[Proceed ]  [  Quit  ]

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

Figure 4.16. PhotoRec Select a media dialog

4. Now we have the Partition selection dialog box. In our case, we have only one partition of unknown type - a perfect example for file carving.



```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk X:\52.E01 - 45 GB / 42 GiB (RO)

     Partition                  Start        End    Size in sectors
>   P Unknown                  0   0  1  5543 138 40    89057028



>[ Search ]  [Options ]  [File Opt]  [  Quit  ]
                              Start file recovery
```

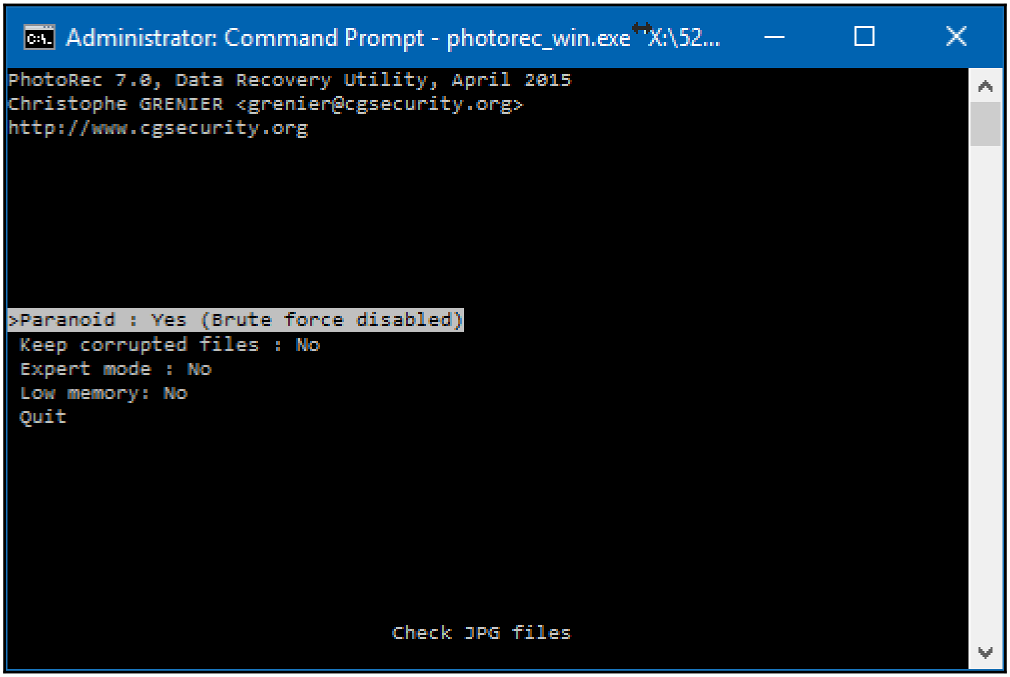
Figure 4.17. PhotoRec Partition selection dialog

5. Also, four options are seen at the bottom:

- **Search** - to start recovery
- **Options** - to modify recovery options
- **File Opt** - to modify file types to be recovered
- **Quit** - to cancel recovery

6. Let's go to **Options**. Here, we have the following:

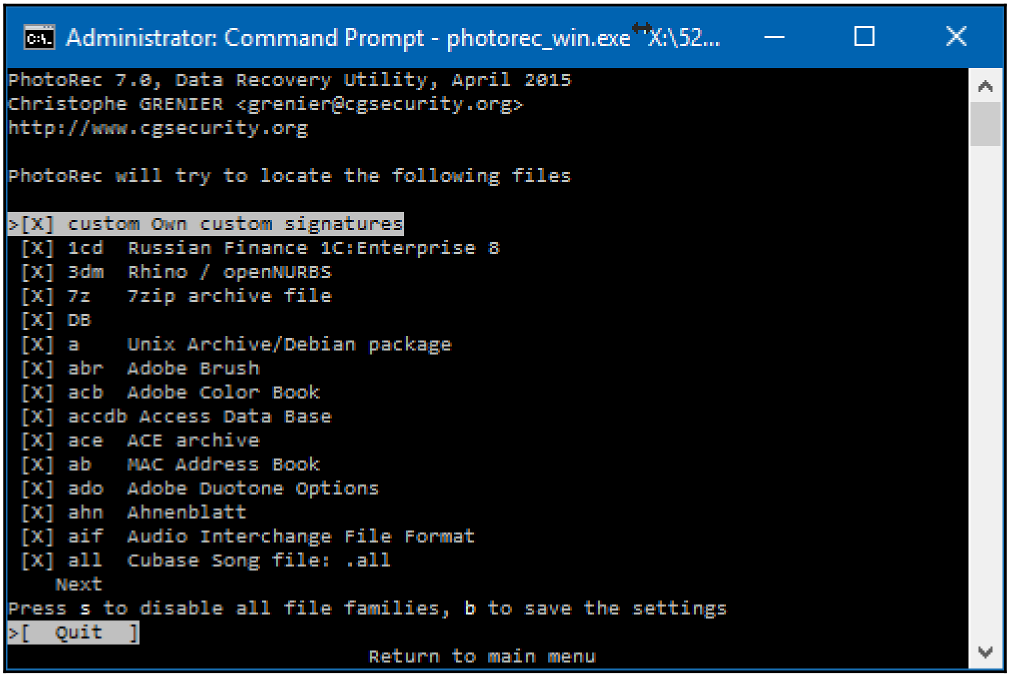
   - **Paranoid** - if enabled, verifies recovered files, and invalid files are rejected. Another option here, **bruteforce**, if enabled, tries to recover fragmented JPG files.
   - **Keep corrupted files** - if enabled, keeps invalid files. Use it if you want to try to repair them with other tools.
   - **Expert mode** - if enabled, allows an examiner to force the block size and the offset.
   - **Low memory** - use it if your workstation doesn't have enough memory to avoid recovery crashes.



```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org




>Paranoid : Yes (Brute force disabled)
 Keep corrupted files : No
 Expert mode : No
 Low memory: No
 Quit




                                Check JPG files
```

Figure 4.18. PhotoRec Options

7. Now let's check **File Opt**. Here, we have a long list of file types supported by the tool. Use the *s* button to check all file types or to disable all. Use spacebar if you want to enable or disable some of the types. To save changes use b.

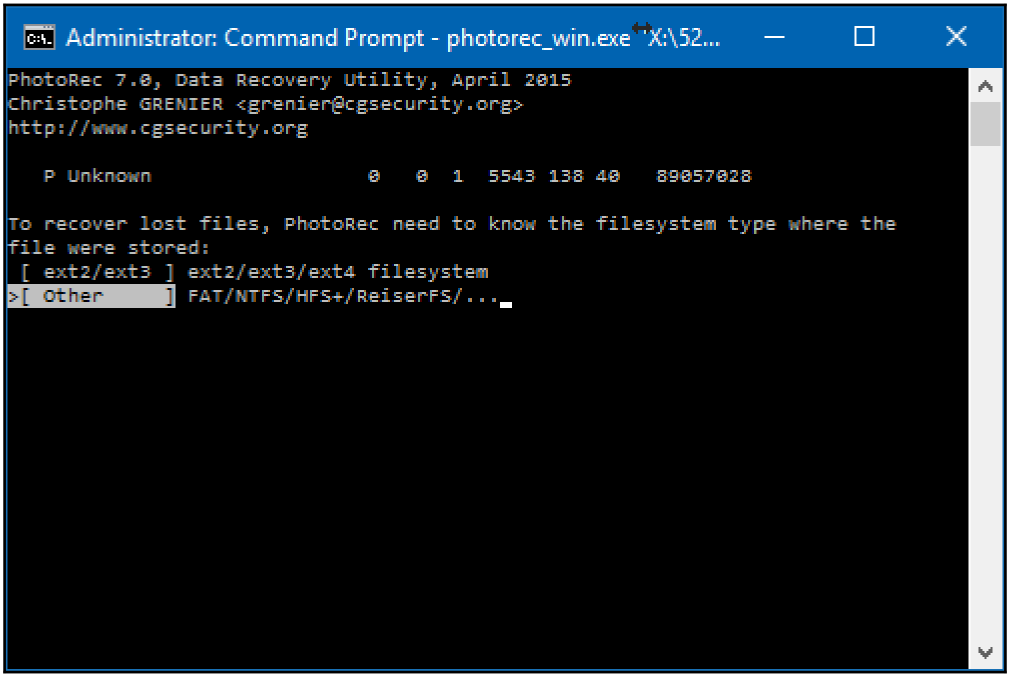


```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec will try to locate the following files

>[X] custom Own custom signatures
 [X] 1cd   Russian Finance 1C:Enterprise 8
 [X] 3dm   Rhino / openNURBS
 [X] 7z    7zip archive file
 [X] DB
 [X] a     Unix Archive/Debian package
 [X] abr   Adobe Brush
 [X] acb   Adobe Color Book
 [X] accdb Access Data Base
 [X] ace   ACE archive
 [X] ab    MAC Address Book
 [X] ado   Adobe Duotone Options
 [X] ahn   Ahnenblatt
 [X] aif   Audio Interchange File Format
 [X] all   Cubase Song file: .all
   Next
Press s to disable all file families, b to save the settings
>[  Quit  ]
                              Return to main menu
```

Figure 4.19. PhotoRec File Opt option

Now we have looked through the available options, and are ready to start recovery.

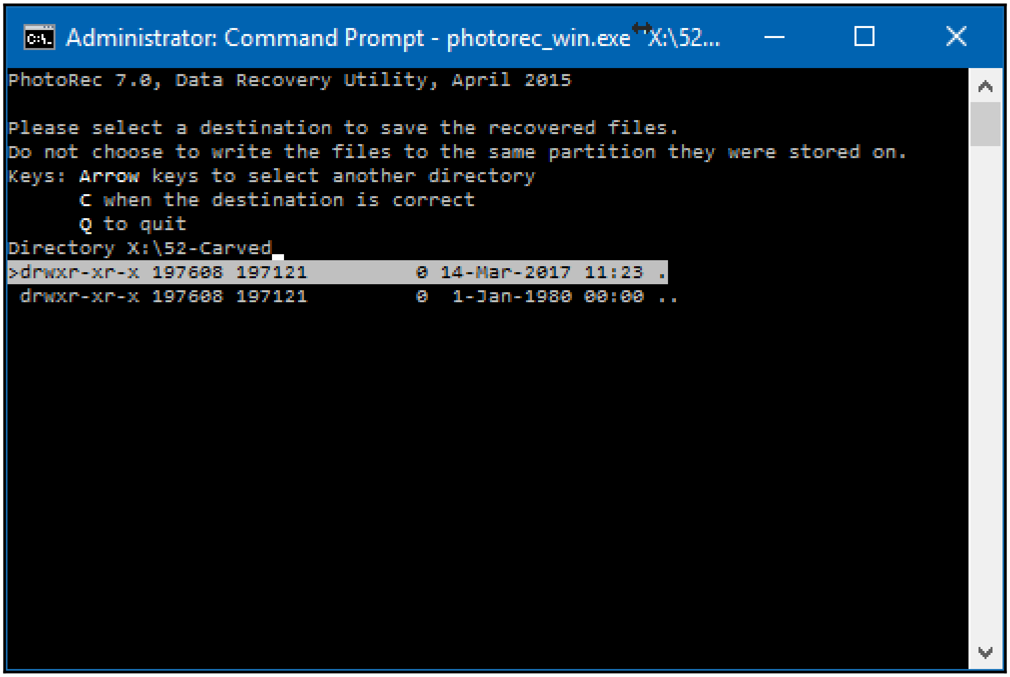
8. Choose **Search** and press *Enter*. It's time to choose the file system type. We know that there are only two options, and that there are no EXT partitions on our image, so we choose **Other**.



```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

   P Unknown                  0   0  1  5543 138 40   89057028

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
 [ ext2/ext3 ] ext2/ext3/ext4 filesystem
>[ Other     ] FAT/NTFS/HFS+/ReiserFS/...
```

Figure 4.20. PhotoRec Filesystem type dialog

9. Now we need to choose the destination path for the files being recovered. We recommend creating one before starting the file carving process. In our case, the destination folder is `X:52-Carved`, as you can see in the following figure:



```
PhotoRec 7.0, Data Recovery Utility, April 2015

Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory X:\52-Carved
>drwxr-xr-x 197608 197121         0 14-Mar-2017 11:23 .
 drwxr-xr-x 197608 197121         0  1-Jan-1980 00:00 ..
```

Figure 4.21. PhotoRec Select destination dialog

10. Use the *C* button to start the file carving process.
11. Once the process is finished, you will have one or more folders (`recup_dir.1`, `recup_dir.2`...) with recovered files. It's important to note that these folders can be accessed before the recovery is finished.

How it works...

PhotoRec reads the data source sector by sector, and finds the first ten files. It uses them to calculate the block/cluster size after each block is checked by the tool against a signature database.

If the file system is not corrupted, PhotoRec can get the block/cluster size from volume boot record, or superblock.

See more

The PhotoRec download page: `http://www.cgsecurity.org/wiki/TestDisk_Download`

The PhotoRec wiki page: `http://www.cgsecurity.org/wiki/PhotoRec`

5

Windows Shadow Copies Analysis

In this chapter, we will cover the following recipes:

- Browsing and copying files from VSCs on a live system with ShadowCopyView
- Mounting VSCs from disk images with VSSADMIN and MKLINK
- Processing and analyzing VSC data with Magnet AXIOM

Introduction

Shadow copies, also known as volume shadow copies, are backup copies of Windows files that are taken during the normal course of use of a machine running on NTFS. For the average computer user, shadow copies may be familiar, as they are what make it possible to create Windows backups, or to perform system restores when something goes wrong.

These have obvious applications for digital forensic practitioners, particularly in cases where a suspect may have tried to delete evidence from a machine. By restoring the system to its previous state, or by using forensic tools to uncover files that are saved in shadow copy locations, forensic practitioners may be able to deduce information that an individual has tried to hide.

However, the presence of shadow copies and the ability forensic investigators have to uncover the information contained within them does not necessarily mean that useful information will be obtained. Many files will simply contain information that is irrelevant to the case. Even when shadow copies of useful files are restored, the version the investigator can see is only a snapshot of the file. In other words, the forensic analyst will only be able to see a single version of a file, rather than any changes that may have been made. Shadow copies are frequently overwritten by the system, and it is possible in most versions of Windows to turn off the ability to create them, which means they are not a failsafe fallback option. Having said that, the ability to locate, restore, and comprehend the data contained within volume shadow copies is an important part of a digital forensic investigator’s toolkit. In this chapter, we will demonstrate a few methods that will help you get to grips with shadow copies analysis.

Browsing and copying files from VSCs on a live system with ShadowCopyView

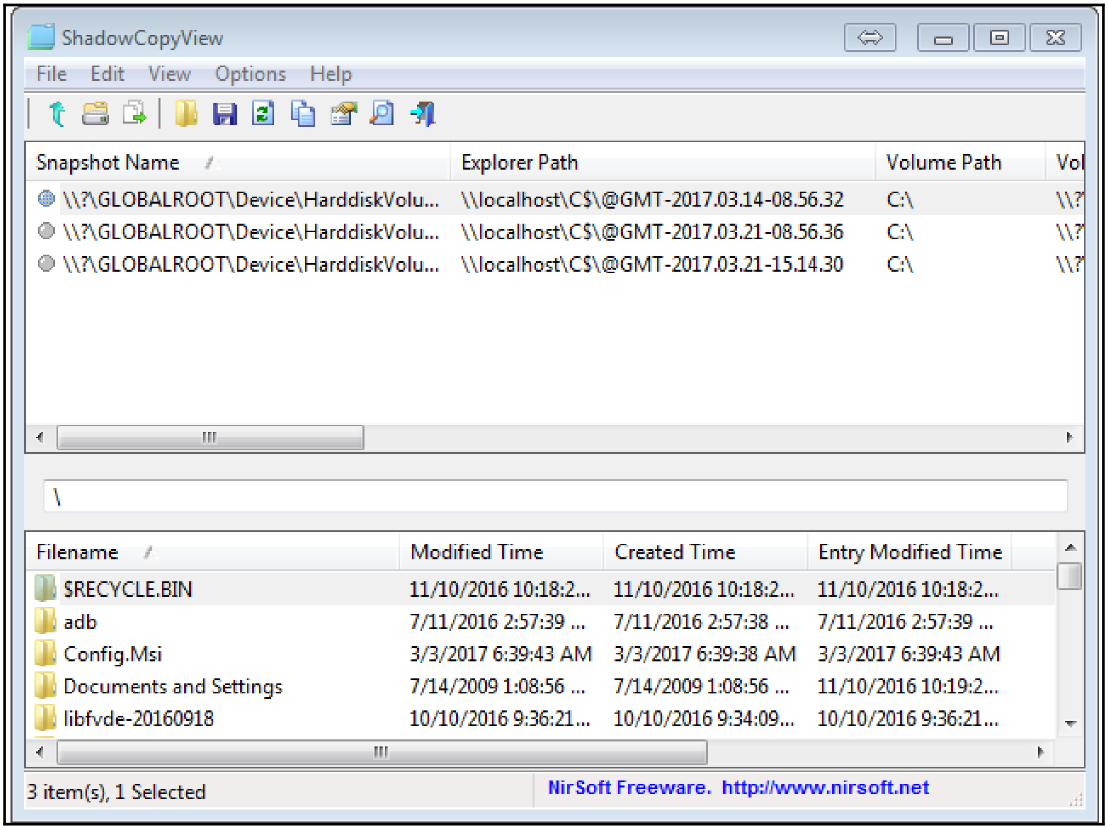
ShadowCopyView is a simple tool developed by **NirSoft** (remember this name! They have developed lots of small free tools which are extremely useful for computer forensics), which enables digital forensic examiners to browse snapshots created by the Windows Volume Shadow Copy Service. It supports even the most recent Windows versions (Windows 10, for example), and can be kept on your favorite USB drive, which is very important for live forensics and incident response.

Getting ready

Go to NirSoft's website and click on the **All Utilities** link on the left. Scroll down the page, find the **ShadowCopyView** link, and click it. At the time of writing, the most recent version of the tool is 1.05. Scroll down and you will find two download links: 32-bit and 64-bit versions. We recommend that you download both, and use them depending on the target system. Unpack the archives you downloaded to your flash drive, and you are ready to go.

How to do it...

Connect your flash drive to the target system. In our case, it's Windows 7 x64, so we will use the 64-bit version of ShadowCopyView. The tool detects available VSCs automatically. In our case we have three VSCs available, as you can see in the following figure:



Snapshot Name	Explorer Path	Volume Path	Vol
\\?\GLOBALROOT\Device\HarddiskVolu...	\\localhost\C$\@GMT-2017.03.14-08.56.32	C:\	\\?
\\?\GLOBALROOT\Device\HarddiskVolu...	\\localhost\C$\@GMT-2017.03.21-08.56.36	C:\	\\?
\\?\GLOBALROOT\Device\HarddiskVolu...	\\localhost\C$\@GMT-2017.03.21-15.14.30	C:\	\\?

\

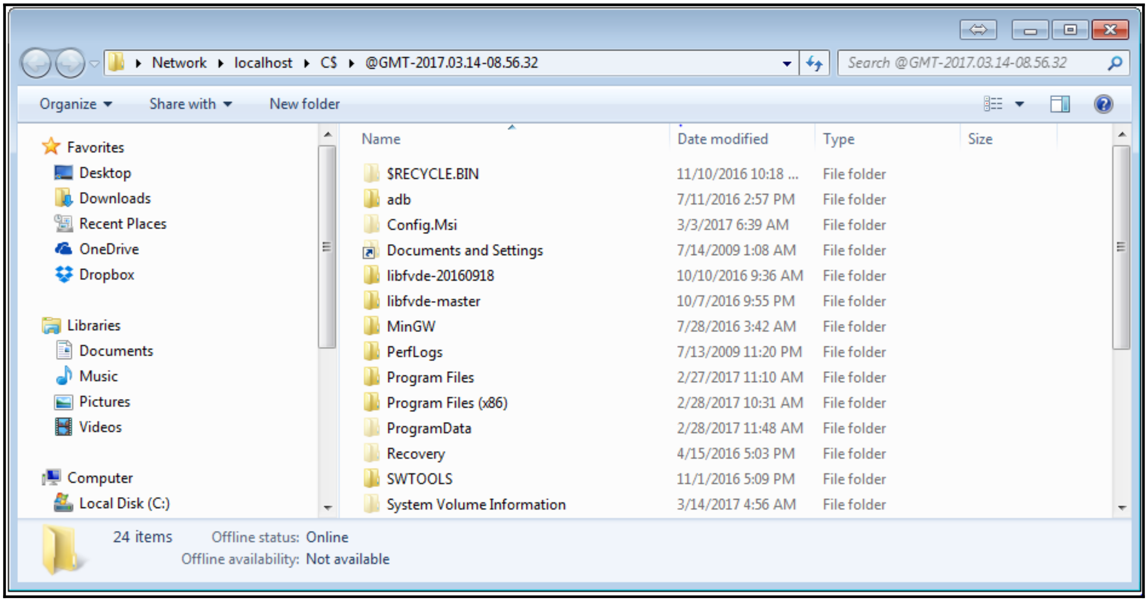
Filename	Modified Time	Created Time	Entry Modified Time
$RECYCLE.BIN	11/10/2016 10:18:2...	11/10/2016 10:18:2...	11/10/2016 10:18:2...
adb	7/11/2016 2:57:39 ...	7/11/2016 2:57:38 ...	7/11/2016 2:57:39 ...
Config.Msi	3/3/2017 6:39:43 AM	3/3/2017 6:39:38 AM	3/3/2017 6:39:43 AM
Documents and Settings	7/14/2009 1:08:56 ...	7/14/2009 1:08:56 ...	11/10/2016 10:19:2...
libfvde-20160918	10/10/2016 9:36:21...	10/10/2016 9:34:09...	10/10/2016 9:36:21...

3 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

Figure 5.1. Volume Shadow Copies detected by ShadowCopyView

The main window of the tool consists of two panes. The first pane displays information about detected shadow copies, including name, **Explorer path**, **Volume path**, **Created Time**, and so on. The **Explorer path** means you can browse shadow copies in Windows Explorer.

1. Right-click on the VSC you want to browse in Explorer and choose **Open In Windows Explorer,** or just press **F2**. Now it's open in Windows Explorer, as you can see in the following figure:



Name	Date modified	Type	Size
$RECYCLE.BIN	11/10/2016 10:18 ...	File folder	
adb	7/11/2016 2:57 PM	File folder	
Config.Msi	3/3/2017 6:39 AM	File folder	
Documents and Settings	7/14/2009 1:08 AM	File folder	
libfvde-20160918	10/10/2016 9:36 AM	File folder	
libfvde-master	10/7/2016 9:55 PM	File folder	
MinGW	7/28/2016 3:42 AM	File folder	
PerfLogs	7/13/2009 11:20 PM	File folder	
Program Files	2/27/2017 11:10 AM	File folder	
Program Files (x86)	2/28/2017 10:31 AM	File folder	
ProgramData	2/28/2017 11:48 AM	File folder	
Recovery	4/15/2016 5:03 PM	File folder	
SWTOOLS	11/1/2016 5:09 PM	File folder	
System Volume Information	3/14/2017 4:56 AM	File folder	

24 items   Offline status: Online
Offline availability: Not available

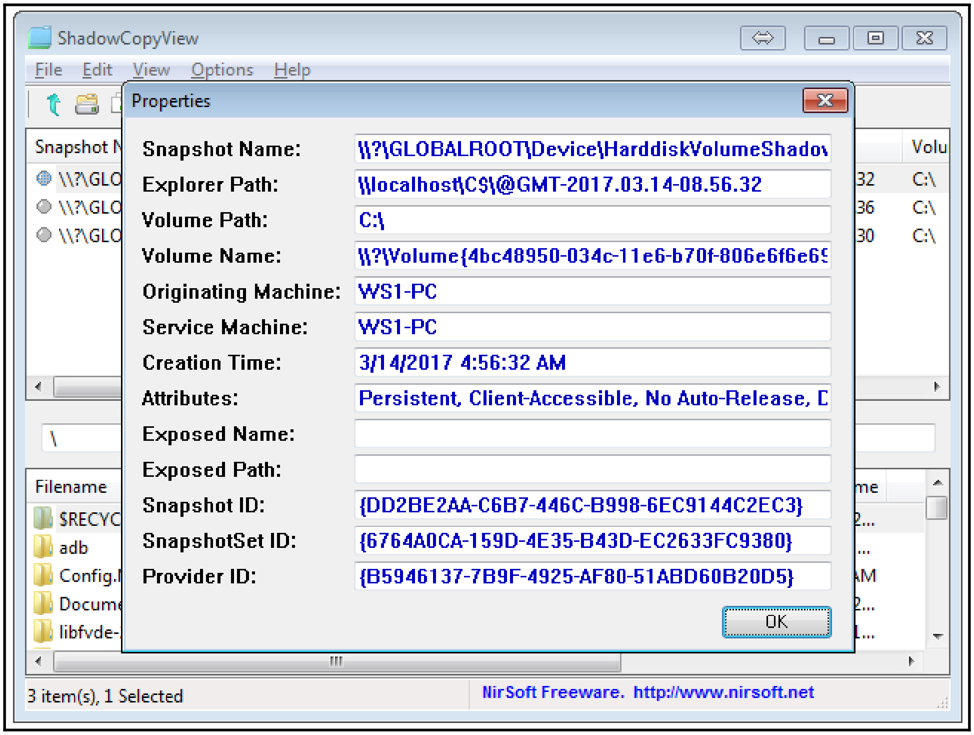
Figure 5.2. A Volume Shadow Copy opened in Windows Explorer

Now, let's get back to ShadowCopyView. The second pane enables you to browse available shadow copies. Using this pane, you can export both files and folders.

2. All you need to do is to right-click a file or a folder, and select the **Copy Selected Files To...** option or just press **F8**.
3. There are some other useful options you can use. For example, if you prefer timestamps in the UTC (Coordinated Universal Time) time standard, you can use the **GMT** (**Greenwich Mean Time**) time zone. To do this, go to the **Options** menu and select **Show Time In GMT**.

UTC or Coordinated Universal Time is the primary standard by which the world regulates clocks and time. For example, most parts of European Russia use UTC +3 hours.

4. Also, if you want to see the whole properties list of a shadow copy, you can right-click it and choose the **Properties** option, or just press *Alt* + *Enter*. Now you see all the properties in one window, as in the following figure:



Snapshot Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadov

Explorer Path: \\localhost\C$\@GMT-2017.03.14-08.56.32

Volume Path: C:\

Volume Name: \\?\Volume{4bc48950-034c-11e6-b70f-806e6f6e6

Originating Machine: WS1-PC

Service Machine: WS1-PC

Creation Time: 3/14/2017 4:56:32 AM

Attributes: Persistent, Client-Accessible, No Auto-Release, D

Exposed Name:

Exposed Path:

Snapshot ID: {DD2BE2AA-C6B7-446C-B998-6EC9144C2EC3}

SnapshotSet ID: {6764A0CA-159D-4E35-B43D-EC2633FC9380}

Provider ID: {B5946137-7B9F-4925-AF80-51ABD60B20D5}

3 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Figure 5.3. A Volume Shadow Copy's properties

And the last very useful feature we want to tell you about is keyword searching.

5. Go to **Edit - Find**, or just press *Ctrl* + *F*, and you will see the **Find** window, as in the following figure:

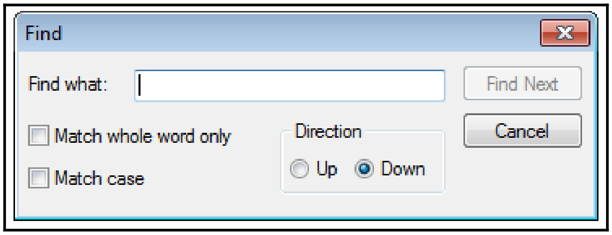


Figure 5.4. ShadowCopyView Find window

6. As you can see, you also have two options to tick. Tick the first one if hits must include the whole word only, tick the second if it is important that results are returned in uppercase or lowercase letters.

How it works...

ShadowCopyView detects available Volume Shadow Copies, enabling a computer forensic examiner to browse them both via the tool and Windows Explorer, and also allows them to search for and export files and folders.

See also

The NirSoft website: `http://www.nirsoft.net/`

The ShadowCopyView download page: `http://www.nirsoft.net/utils/shadow_copy_view.html`

Mounting VSCs from disk images with VSSADMIN and MKLINK

VSSADMIN is a built-in Windows command-line tool capable of displaying Volume Shadow Copies. You can use it not only on a running Windows system, but also on disk images. In this recipe, we will show you how to do it.

Getting ready

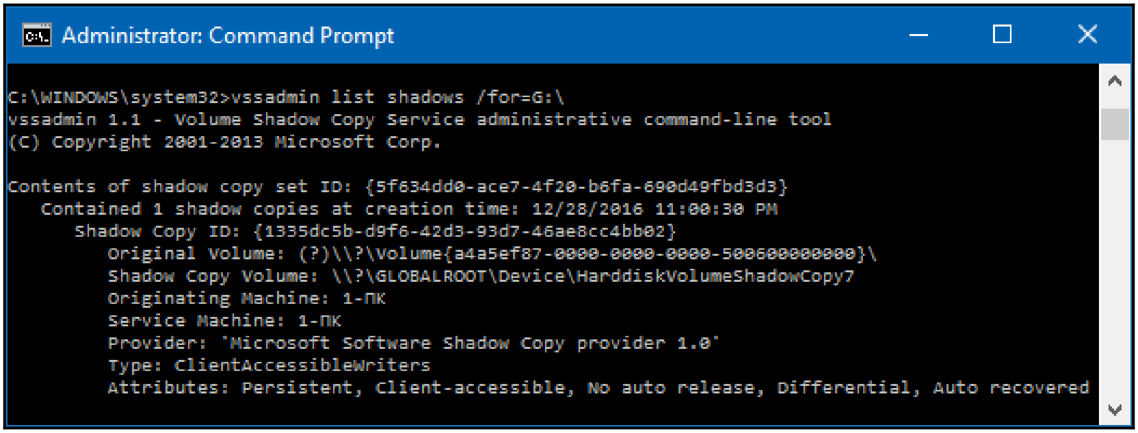
As the tool we are going to use is built-in, there is no need for installation: if you are using Windows, you already have it. So all you need is to mount a forensic image, and you already know how to do this from `Chapter 3`, *Windows Drive Acquisition*. As soon as the image is mounted, you are ready to go.

How to do it...

The steps to mount VSCs from disk images using VSSADMIN and MKLINK are as follows:

1. Start Windows Command Prompt (don't forget to run it as Administrator). In our case, the boot partition is mounted as `G:\ drive`, so we use the following command:

```
vssadmin list shadows /for=G:\
```



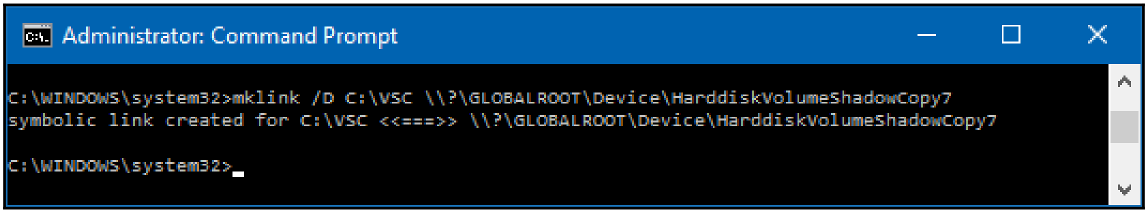
```
C:\WINDOWS\system32>vssadmin list shadows /for=G:\
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {5f634dd0-ace7-4f20-b6fa-690d49fbd3d3}
   Contained 1 shadow copies at creation time: 12/28/2016 11:00:30 PM
      Shadow Copy ID: {1335dc5b-d9f6-42d3-93d7-46ae8cc4bb02}
         Original Volume: (?)\\?\Volume{a4a5ef87-0000-0000-0000-500600000000}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
         Originating Machine: 1-ПК
         Service Machine: 1-ПК
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered
```

Figure 5.5. vssadmin list shadows /for=G:\ command output

As you can see in the preceding figure, our forensic image contains a shadow copy.

2. The most important part of its properties for us is **Shadow Copy Volume**, in our case it's `\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7`. Now we are ready to use MKLINK to mount the shadow copy we found. Use the following command:

```
mklink /D C:\VSC \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
```



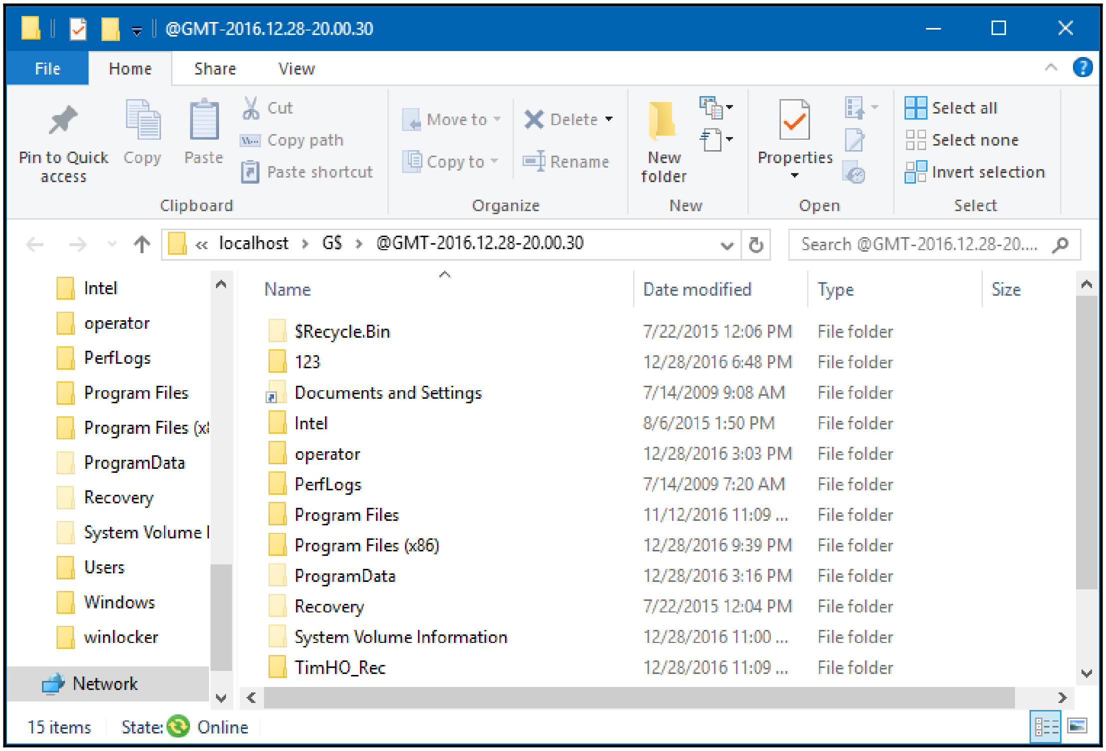
```
C:\WINDOWS\system32>mklink /D C:\VSC \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7
symbolic link created for C:\VSC <<===>> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7

C:\WINDOWS\system32>
```

Figure 5.6. mklink /D C:\VSC \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7 command output

MKLINK creates a folder (you should choose its name and location, and type it in as part of the command) and mounts the shadow copy to it, so you can browse it like a normal folder. Don't forget the **/D** switch — we need it to create a directory symbolic link, not a file.

3. There is another way to use Windows Explorer for VSC browsing. We need to get a VSC path in the following format `\\localhost\G$\@GMT-2016.12.28-20.00.30`

The first part of the path, `\\localhost\`, will be always the same. The next part depends on the drive letter of the boot partition. As you will remember, in our case it's `G:\`, so in the path it is `G$`. For example, if you have `H:\`, it's `H$`, and so on. The last part is based on the VSC's creation time. You can get it from the VSSADMIN output, but it must be converted into GMT. Now just type it as a path in Windows Explorer, and the shadow copy will be available for examination, as in the following figure:



« localhost › G$ › @GMT-2016.12.28-20.00.30

Search @GMT-2016.12.28-20....

Name	Date modified	Type	Size
$Recycle.Bin	7/22/2015 12:06 PM	File folder	
123	12/28/2016 6:48 PM	File folder	
Documents and Settings	7/14/2009 9:08 AM	File folder	
Intel	8/6/2015 1:50 PM	File folder	
operator	12/28/2016 3:03 PM	File folder	
PerfLogs	7/14/2009 7:20 AM	File folder	
Program Files	11/12/2016 11:09 ...	File folder	
Program Files (x86)	12/28/2016 9:39 PM	File folder	
ProgramData	12/28/2016 3:16 PM	File folder	
Recovery	7/22/2015 12:04 PM	File folder	
System Volume Information	12/28/2016 11:00 ...	File folder	
TimHO_Rec	12/28/2016 11:09 ...	File folder	

15 items State: Online

Figure 5.7. A Volume Shadow Copy opened in Windows Explorer

How it works...

VSSADMIN displays available Volume Shadow Copies on a mounted forensic image. MKLINK creates a symbolic link to the shadow copy, so a digital forensic examiner can browse it in Windows Explorer.

See also

The VSSADMIN page at Misrosoft TechNet: `https://technet.microsoft.com/en-us/library/cc754968(v=ws.11).aspx`

The MKLINK page at Microsoft TechNet: `https://technet.microsoft.com/en-us/library/cc753194(v=ws.11).aspx`

Processing and analyzing VSC data with Magnet AXIOM

Magnet AXIOM is an all-in-one digital forensics tool by Magnet Forensics, capable of extracting (acquiring) and processing data from both computers and mobile devices. It supports lots of Windows forensic artifacts, including extracting data from Windows Volume Shadow Copies.

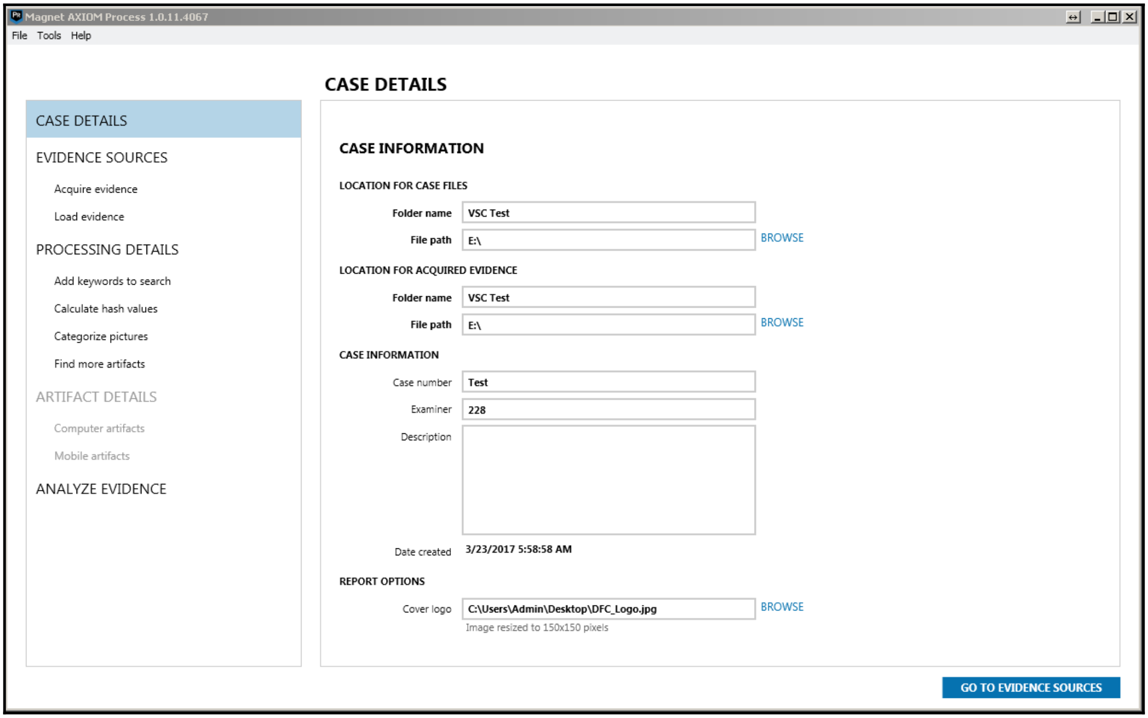
Getting ready

At the time of writing, Magnet Forensics provides a fully functional 30-day free trial version of Magnet AXIOM. All you need to do is go to Magnet Forensics' website and click on the **TRY NOW** button. Fill in the form, including your first name, last name, email address, phone number, state or province, country, and so on and click on **REQUEST A FREE TRIAL**. Make sure you type your real email: your trial key and download link will be sent to this address. Once you get it, download the installer and follow its instructions. You are ready to go!

How to do it...

The steps to process and analyze data using Magnet AXIOM are as follows:

1. Start the Magnet AXIOM Process.
2. The first window you will see is **CASE DETAILS**, as you can see in the following figure:



CASE DETAILS

CASE INFORMATION

LOCATION FOR CASE FILES

Folder name: VSC Test
File path: E:\

LOCATION FOR ACQUIRED EVIDENCE

Folder name: VSC Test
File path: E:\

CASE INFORMATION

Case number: Test
Examiner: 228
Description:
Date created: 3/23/2017 5:58:58 AM

REPORT OPTIONS

Cover logo: C:\Users\Admin\Desktop\DFC_Logo.jpg
Image resized to 150x150 pixels

Figure 5.8. Magnet AXIOM CASE DETAILS window

Here, we have four main parts:

- **LOCATION FOR CASE FILES** - Here, you should choose the **Folder name** and **File path** being created during processing.
- **LOCATION FOR ACQUIRED EVIDENCE** - If you plan to acquire drives or mobile devices via AXIOM, choose the **Folder name** and **File path** for them, or just choose the same path as for case files.
- **CASE INFORMATION** - Type in your case number, your name, and the case description.
- **REPORT OPTIONS** - If you have your own logo or company logo, you can choose it by clicking **BROWSE**. Make sure the image is square, because it will be resized to 150x150 pixels.

3. Once you have filled in all the fields, you can click **GO TO EVIDENCE SOURCES**. You can see the **EVIDENCE SOURCES** window shown in the following figure:

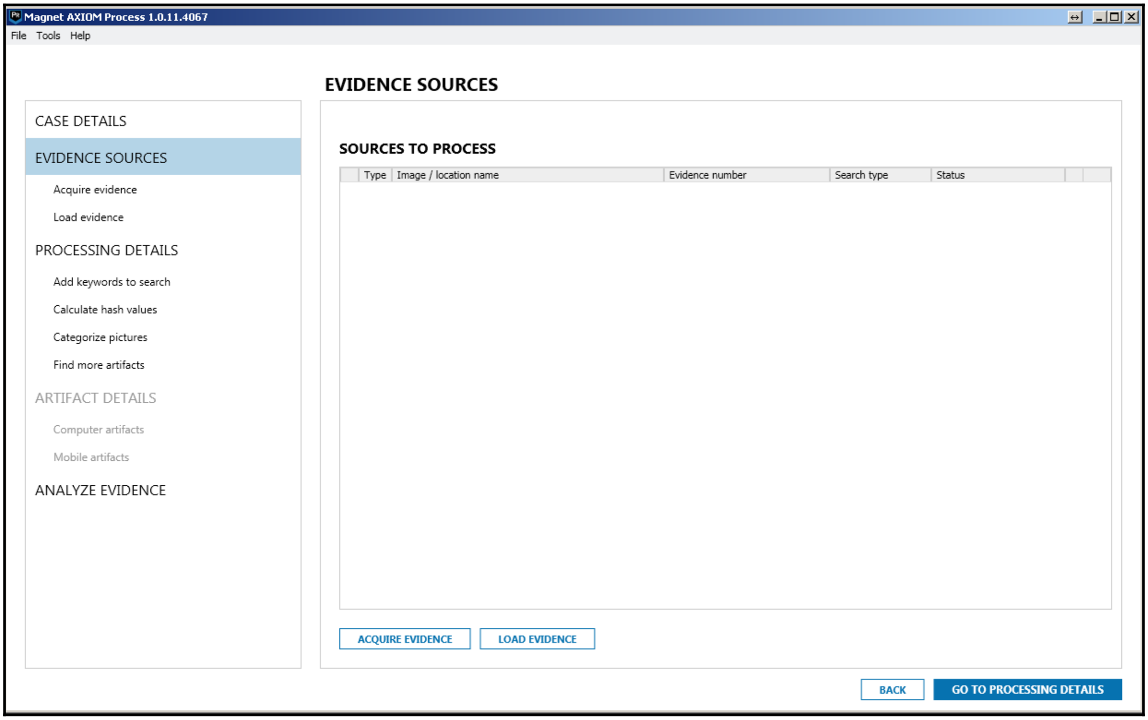


Figure 5.9. Magnet AXIOM EVIDENCE SOURCES window

Here, we have two options: ACQUIRE EVIDENCE and LOAD EVIDENCE.

4. We are going to use an image we acquired previously, so our choice is the **LOAD EVIDENCE** button. You can use one of the images you acquired in the previous recipes.

5. The next window is **LOAD EVIDENCE**, as you can see in the following figure:

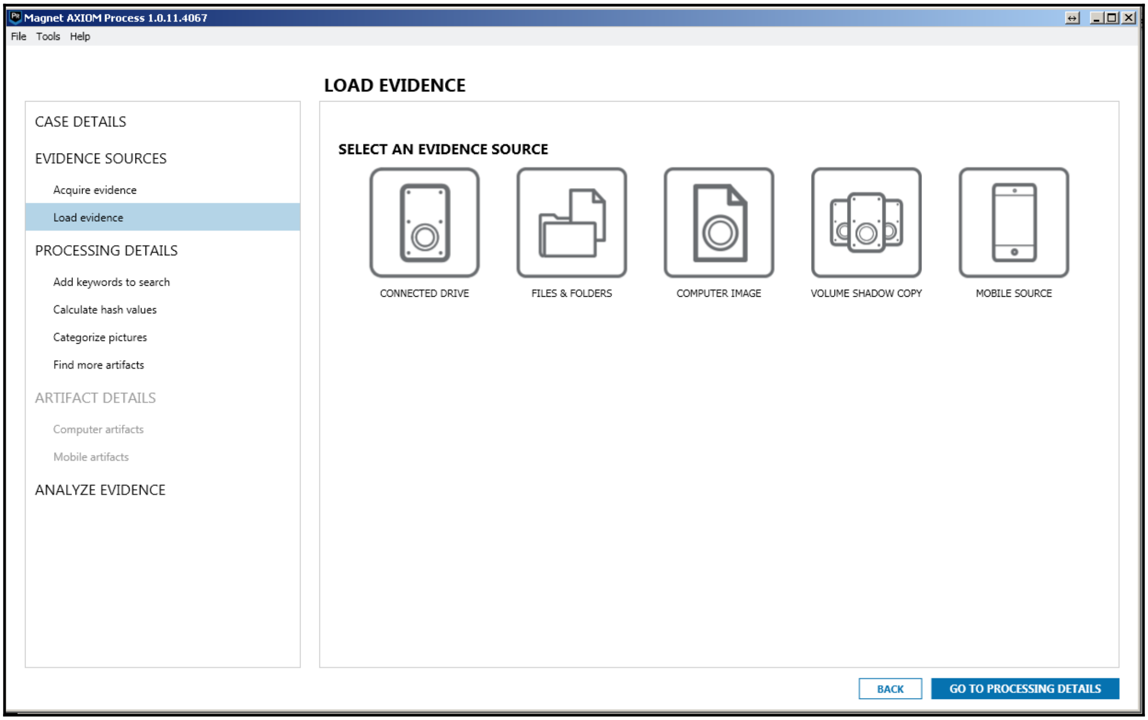
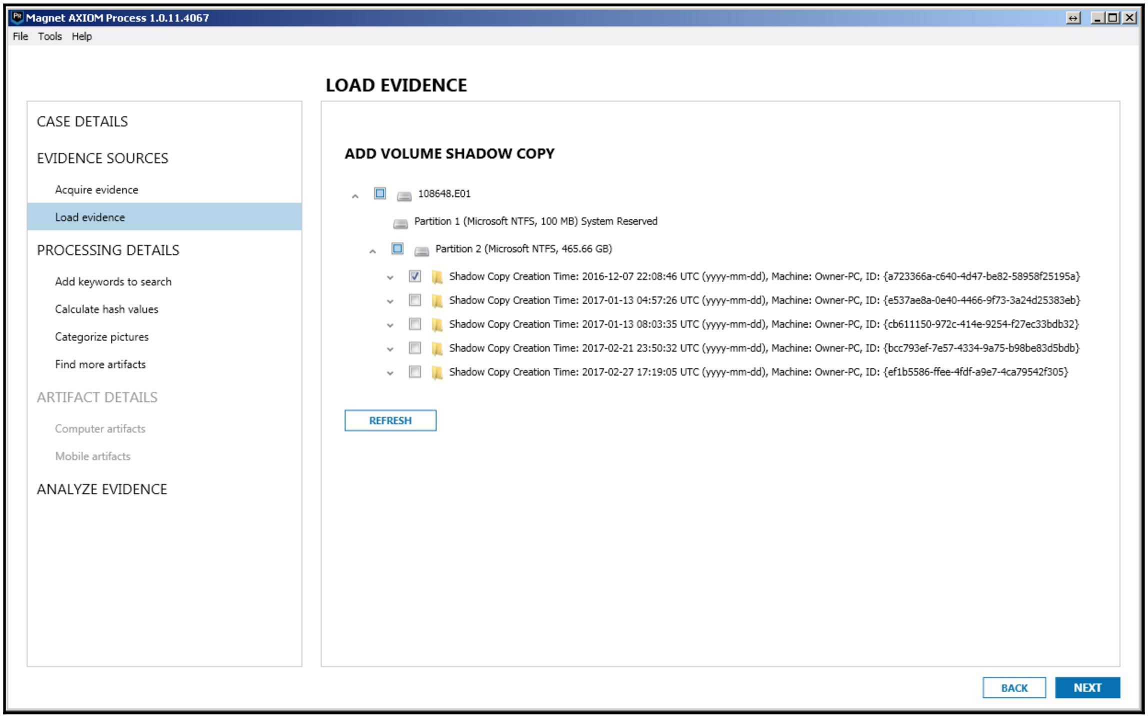


Figure 5.10. Magnet AXIOM LOAD EVIDENCE window

6. Here, we have a VOLUME SHADOW COPY option - click it. Now we have two more options: **DRIVE** and **IMAGE**.

7. As we noted earlier, we are going to use an image. Once you choose it, you can see the list of shadow copies available on the image, as in the following figure:



LOAD EVIDENCE

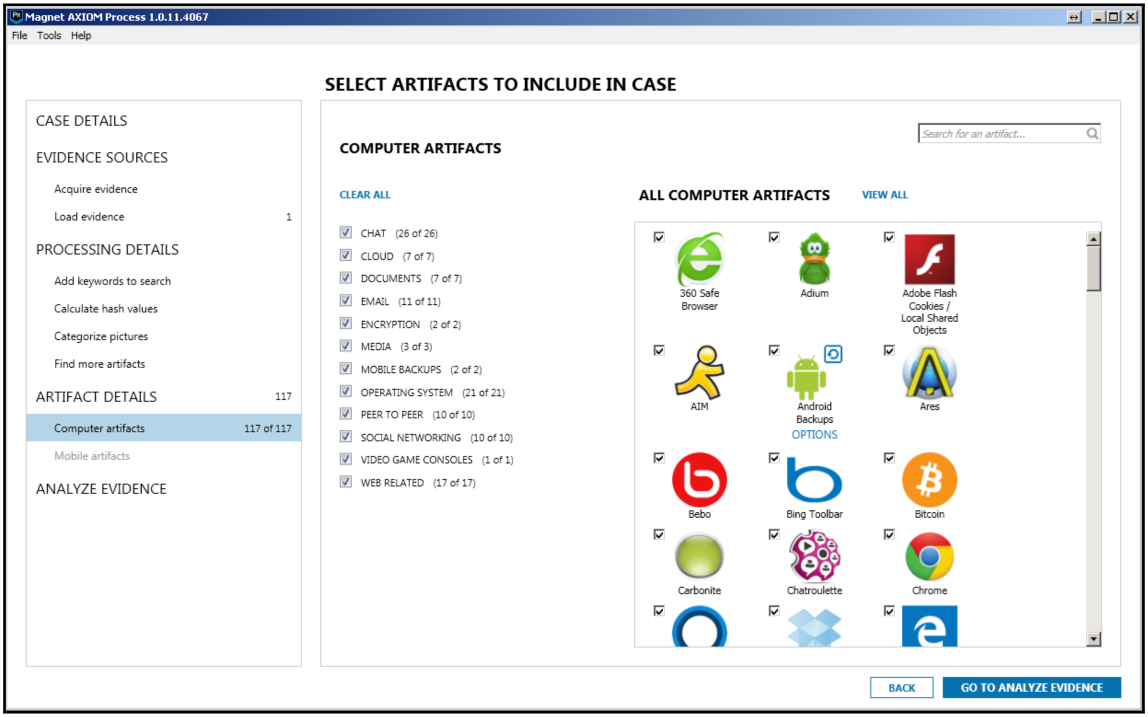
ADD VOLUME SHADOW COPY

- □ 108648.E01
  - Partition 1 (Microsoft NTFS, 100 MB) System Reserved
  - □ Partition 2 (Microsoft NTFS, 465.66 GB)
    - ☑ Shadow Copy Creation Time: 2016-12-07 22:08:46 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {a723366a-c640-4d47-be82-58958f25195a}
    - □ Shadow Copy Creation Time: 2017-01-13 04:57:26 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {e537ae8a-0e40-4466-9f73-3a24d25383eb}
    - □ Shadow Copy Creation Time: 2017-01-13 08:03:35 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {cb611150-972c-414e-9254-f27ec33bdb32}
    - □ Shadow Copy Creation Time: 2017-02-21 23:50:32 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {bcc793ef-7e57-4334-9a75-b98be83d5bdb}
    - □ Shadow Copy Creation Time: 2017-02-27 17:19:05 UTC (yyyy-mm-dd), Machine: Owner-PC, ID: {ef1b5586-ffee-4fdf-a9e7-4ca79542f305}

Figure 5.11. Volume Shadow Copies list

8. You can choose one or more shadow copies and go to processing details by clicking **NEXT**. This time, we will skip this step and go straight to artifacts details (click the **GO TO ARTIFACTS DETAILS** button).

As we are working with a shadow copy, the MOBILE ARTIFACTS option is inactive, but we can use the COMPUTER ARTIFACTS option. As in Belkasoft Evidence Center, here we have a wide range of artifacts, as you can see in the following figure:



☑ CHAT (26 of 26)
☑ CLOUD (7 of 7)
☑ DOCUMENTS (7 of 7)
☑ EMAIL (11 of 11)
☑ ENCRYPTION (2 of 2)
☑ MEDIA (3 of 3)
☑ MOBILE BACKUPS (2 of 2)
☑ OPERATING SYSTEM (21 of 21)
☑ PEER TO PEER (10 of 10)
☑ SOCIAL NETWORKING (10 of 10)
☑ VIDEO GAME CONSOLES (1 of 1)
☑ WEB RELATED (17 of 17)

Figure 5.12. Magnet AXIOM SELECT ARTIFACTS TO INCLUDE IN CASE window

9. For testing purposes, we have included all available artifacts in the case. Click the **GO TO ANALYZE EVIDENCE** button, and the **ANALYZE EVIDENCE** button right after that. This will start Magnet AXIOM Examine.
10. Once processing is finished, you will see the results in Magnet AXIOM Examine.

How it works...

Magnet AXIOM scans a drive or an image for available Volume Shadow Copies and uses them as its evidence source. After it has processed all available data in the chosen shadow copies, it extracts forensic artifacts according to the choices made by the examiner.

See also

The Magnet Forensics website: `https://www.magnetforensics.com/`

The Magnet AXIOM free 30-day trial request page: `https://www.magnetforensics.com/try-magnet-axiom-free-30-days/`

Belkasoft Evidence Center: `https://belkasoft.com/ec`

6
Windows Registry Analysis

In this chapter, we will cover the following recipes:

- Extracting and viewing Windows Registry files with Magnet AXIOM
- Parsing Registry files with RegRipper
- Recovering deleted Registry artifacts with Registry Explorer
- Registry analysis with FTK Registry Viewer

Introduction

The Windows Registry is one of the richest sources of digital evidence. You can find lots of extremely useful pieces of information during examination of the Registry hives and keys. Computer configurations, recently visited webpages and opened documents, connected USB devices, and many other artifacts can all be acquired through Windows Registry forensic examination.

The Registry has a tree structure. Each tree consists of keys, and each key may have one or more subkeys and values.

As forensic examiners usually deal with drive images, it's very important to know where these registry files are stored. The first six files are located at `C:\Windows\System32\config`. These files are:

- COMPONENTS
- DEFAULT
- SAM
- SECURITY
- SOFTWARE
- SYSTEM

There are also two files for each user account:

- `NTUSER.DAT`, located at `C:\Users\%Username%\`
- `UsrClass.dat`, located at `C:\Users\%Username%\AppData\Local\Microsoft\Windows`

In this chapter, we will show you how to examine these files with both commercial and open source forensic tools, and how to recover deleted keys, sub keys, and values.

Extracting and viewing Windows Registry files with Magnet AXIOM

You have already learnt a bit about how to use Magnet AXIOM in your forensic examinations, especially if you need to extract and analyze data from shadow copies. But this tool has lots of very useful features, so we will use it in a few more recipes. This time you will learn how to use Magnet AXIOM, and especially its Registry Explorer component, for Windows Registry forensics.

Getting ready

If you are following the recipes in this book one by one, you already have Magnet AXIOM - at least a trial version - installed. If not, refer to *`Chapter 5`*, *Windows Shadow Copies Analysis,* for installation instructions. Once you've installed the tool, you are ready to go.

How to do it...

The steps to be followed for Windows Registry analysis using Magnet AXIOM are as follows:

1. Let's create a new case. Once it has been created and all the fields are filled in, go to evidence sources. Click the **Load evidence** button, and you will see the **SELECT AN EVIDENCE SOURCE** window, like the one in the following figure:

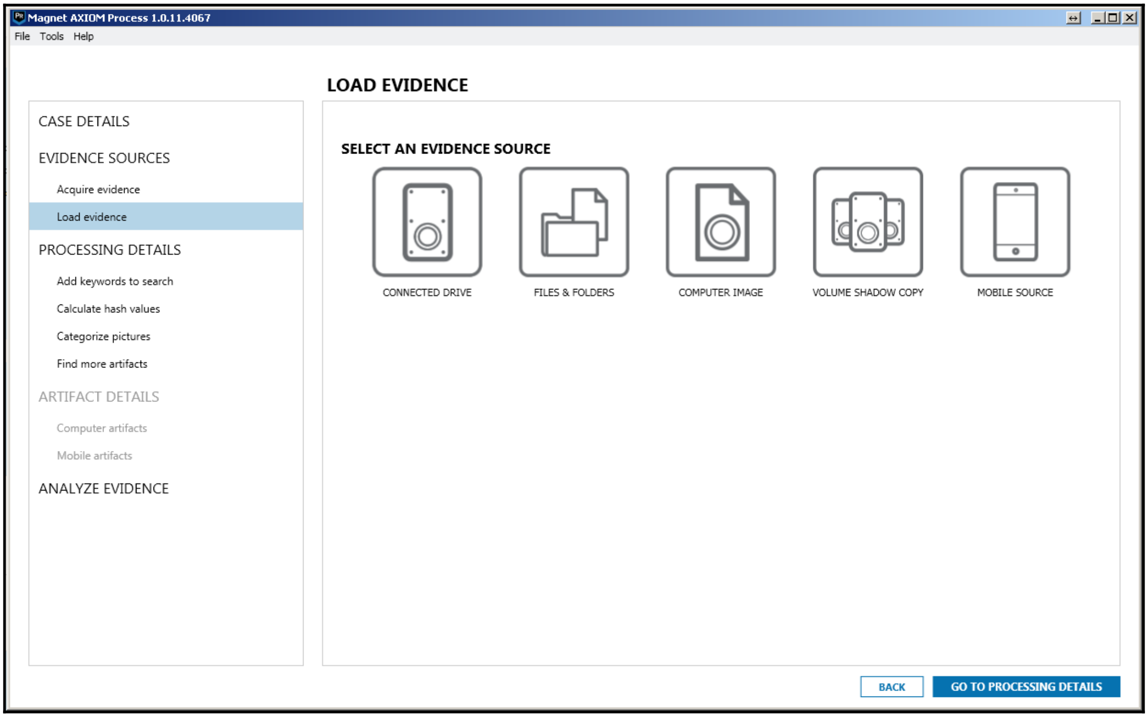
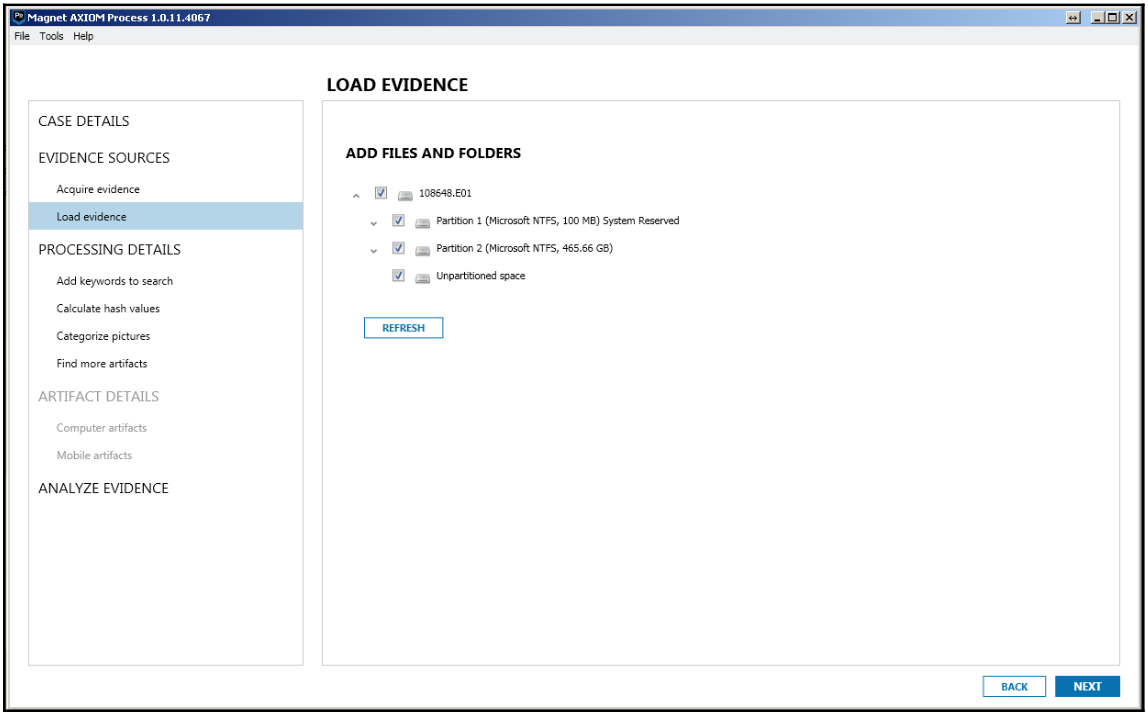


Figure 6.1. Magnet AXIOM SELECT AN EVIDENCE SOURCE window

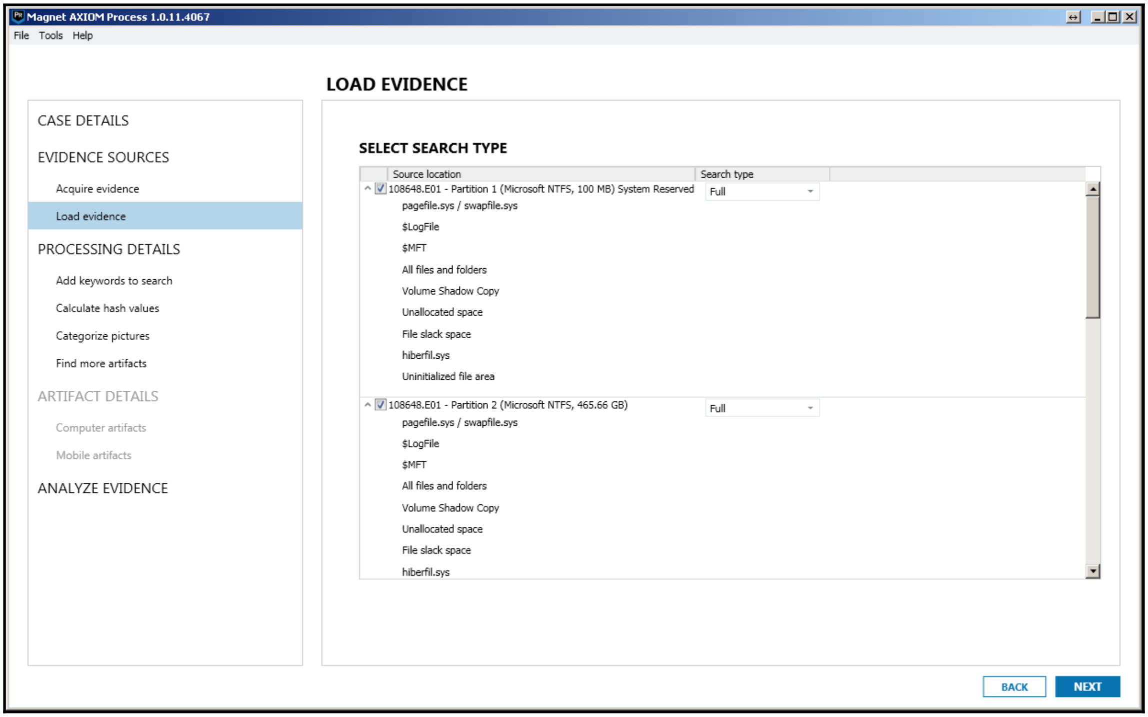
2. This time, let's choose the **COMPUTER IMAGE** option. Again, you can use one of the images you acquired in a previous recipe; both RAW and E01 are supported. Looking at the following figure, we can see that our image contains two partitions and an unpartitioned space.



☑ 108648.E01
☑ Partition 1 (Microsoft NTFS, 100 MB) System Reserved
☑ Partition 2 (Microsoft NTFS, 465.66 GB)
☑ Unpartitioned space

Figure 6.2. Magnet AXIOM ADD FILES AND FOLDERS window

3. You can tick only the main partition (**Partition 2**), or choose all available partitions, as we did. Click **NEXT** and you will be brought to the **SELECT SEARCH TYPE** screen, which you can see in the following figure:



LOAD EVIDENCE

SELECT SEARCH TYPE

Source location	Search type
☑ 108648.E01 - Partition 1 (Microsoft NTFS, 100 MB) System Reserved	Full
pagefile.sys / swapfile.sys	
$LogFile	
$MFT	
All files and folders	
Volume Shadow Copy	
Unallocated space	
File slack space	
hiberfil.sys	
Uninitialized file area	
☑ 108648.E01 - Partition 2 (Microsoft NTFS, 465.66 GB)	Full
pagefile.sys / swapfile.sys	
$LogFile	
$MFT	
All files and folders	
Volume Shadow Copy	
Unallocated space	
File slack space	
hiberfil.sys	

Figure 6.3. Magnet AXIOM SELECT SEARCH TYPE window

4. There are four search types in the Magnet AXIOM process:
    - **Full** - used to extract data from all locations, including unallocated space, shadow copies, and so on.
    - **Quick** - used to extract data from common areas.
    - **Sector level** - this option is very useful for unknown or corrupted file systems, or formatted drives.
    - **Custom** - this option enables the examiner to choose locations. For example, if you want AXIOM to carve unallocated space only, you can choose only this location.

For testing purposes, you can choose all locations, but it will take a lot of time to process it. Also, you can start from Quick type to gather low-hanging fruits. If you don't want to make changes to artifact types, you can go straight to the **ANALYZE EVIDENCE** section. Click the **ANALYZE EVIDENCE** button, and **Magnet AXIOM Examine** will show up.

5. Once data source processing has finished, go to the drop-down menu on the left, like the one you can see in the following figure, and choose the **Registry** option:

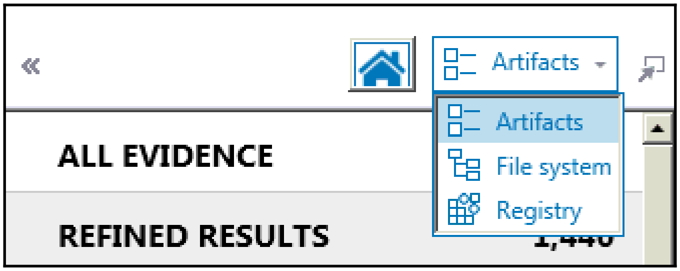


Figure 6.4. Magnet AXIOM Examine navigation pane

6. Once you choose this, you can see all available files containing registry hives on the navigation pane, as in the following figure:

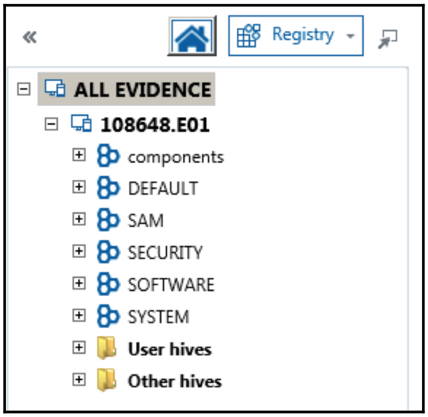
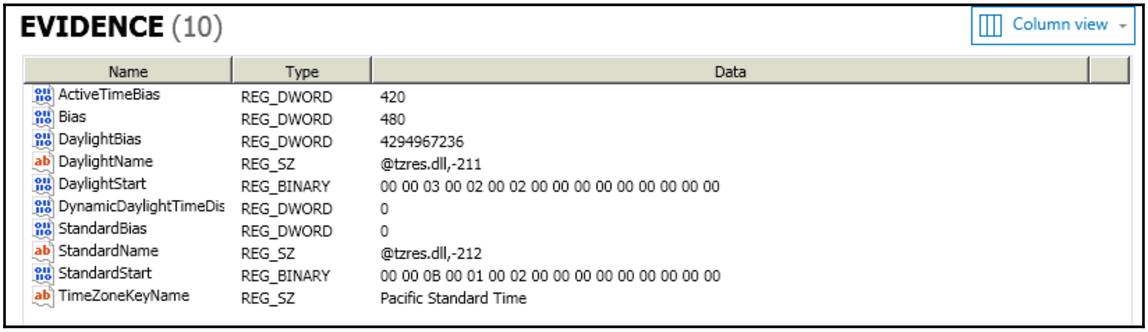


Figure 6.5. AXIOM Registry viewer's navigation pane

7. If you click on the plus sign of a registry file, you can browse its contents, and also see the values on the evidence pane of AXIOM Registry viewer.

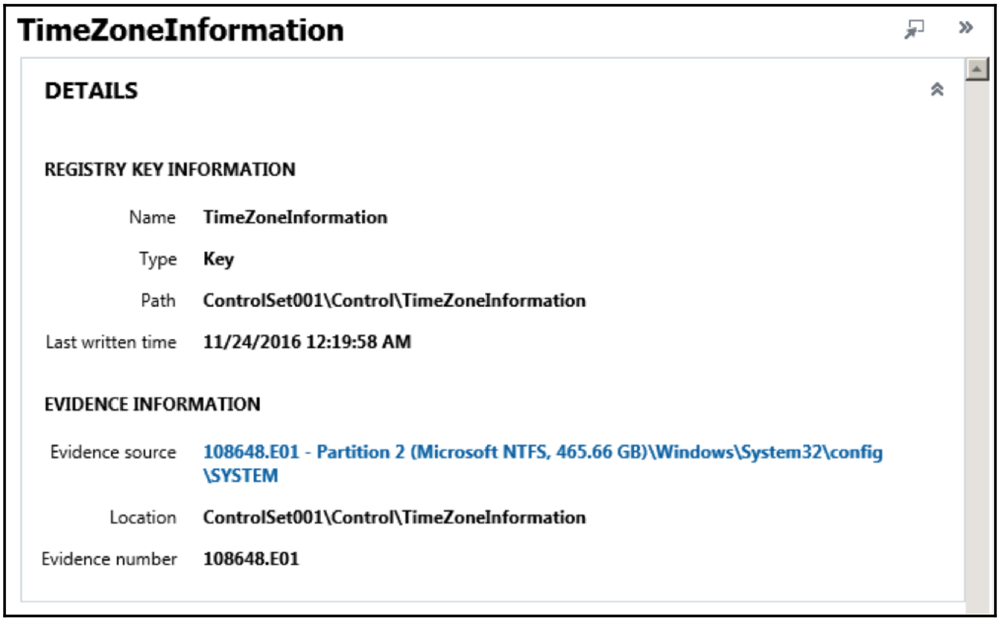


EVIDENCE (10)

Name	Type	Data
ActiveTimeBias	REG_DWORD	420
Bias	REG_DWORD	480
DaylightBias	REG_DWORD	4294967236
DaylightName	REG_SZ	@tzres.dll,-211
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
DynamicDaylightTimeDis	REG_DWORD	0
StandardBias	REG_DWORD	0
StandardName	REG_SZ	@tzres.dll,-212
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Pacific Standard Time

Figure 6.6. AXIOM Registry viewer's evidence pane

8. In the preceding figure, you can see the contents of the **TimeZoneInformation** key. This is a very important key, as it helps examiners to detect the right time zone. More information about the key you are viewing and its source can be found in the **DETAILS** pane, shown in the following figure:



TimeZoneInformation

DETAILS

REGISTRY KEY INFORMATION

Name TimeZoneInformation

Type Key

Path ControlSet001\Control\TimeZoneInformation

Last written time 11/24/2016 12:19:58 AM

EVIDENCE INFORMATION

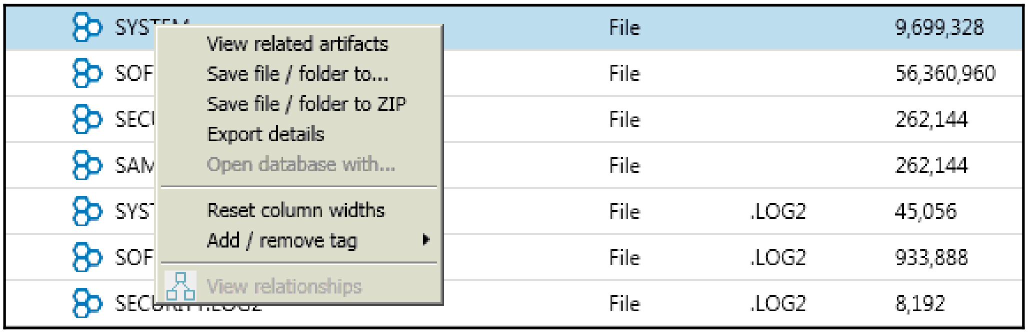
Evidence source 108648.E01 - Partition 2 (Microsoft NTFS, 465.66 GB)\Windows\System32\config \SYSTEM

Location ControlSet001\Control\TimeZoneInformation

Evidence number 108648.E01

Figure 6.7. AXIOM Registry viewer's details pane

9. Look at the **Evidence source**. If you click the blue link, it brings you to the registry file's location and opens it in the file system viewer. Now you can export the registry file. To do this, right-click the file and choose **Save file / folder to...** as shown in the following screenshot:



SYST	File		9,699,328
SOF	File		56,360,960
SECI	File		262,144
SAM	File		262,144
SYS	File	.LOG2	45,056
SOF	File	.LOG2	933,888
SEC	File	.LOG2	8,192

Figure 6.8. Exporting a registry file

10. You can also view the artifacts AXIOM extracted automatically during the processing phase. To do this, right-click the registry file and click **View related artifacts** from the context menu.

Once you have exported the file, you can parse it with other tools. Of course, Magnet AXIOM is a very powerful forensic tool and it extracts lots of data from registry files, but sometimes it's useful to parse them with some other tools, for example, **RegRipper.** We will show you how to do this in the next recipe.

How it works...

Magnet AXIOM collects all available registry files so that a digital forensic examiner can analyze them manually, or export them for parsing with other tools. Also, AXIOM extracts a lot of forensic artifacts from these files automatically, so an examiner can analyze the results in the evidence pane of Magnet AXIOM Examine.

See also

The Magnet AXIOM overview:

`https://www.magnetforensics.com/magnet-axiom/`

Parsing registry files with RegRipper

RegRipper is an open source Windows forensic tool developed by the famous forensicator Harlan Carvey, the author of the *Windows Forensic Analysis* series. It's written in Perl, and has a lot of useful plugins available. Also, digital forensic examiners capable of writing in Perl can create their own plugins for their specific needs.

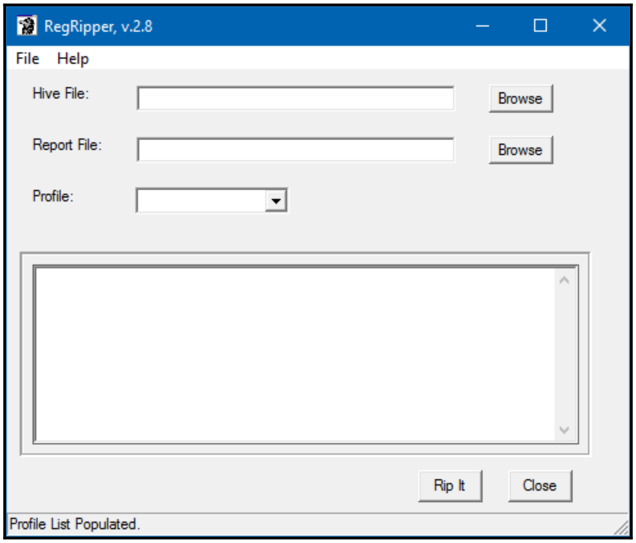
Getting ready

Go to RegRipper's page at Harlan's GitHub, click on the green button (Clone or Download), and choose the **Download ZIP** option. Once the archive is downloaded (in our case it is named **RegRipper2.8-master.zip**), unpack it, and you are ready to go.

How to do it...

The steps for parsing registry files with RegRipper:

1. You already know how to export registry files from disk images, at least with Magnet AXIOM. So, we are sure you have a file to parse with RegRipper. Start `rr.exe`, and you will see a window like the one in the following figure:



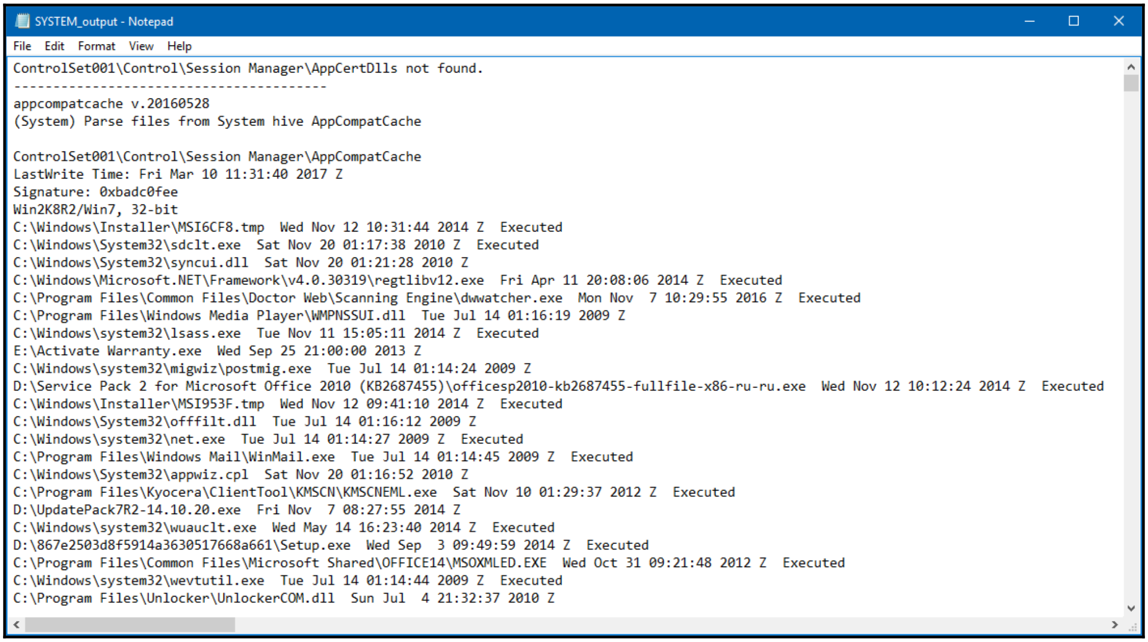
Profile List Populated.

Figure 6.9. RegRipper main window

Here, you have three fields to fill in:

- **Hive File** - Use the Browse button and choose the hive (registry) file you exported previously. In our case, it's **SYSTEM**.
- **Report File** - Use the Browse button and choose a file to save the output (it's in plain text, so a TXT file will do). In our case, the file is called SYSTEM_output.
- **Profile** - Choose the right profile for parsing from the drop-down menu. We are using the SYSTEM file as the source, so our profile of choice is 'system'.

2. Once you've chosen your files and the right profile, you can press the **Rip It** button. As soon as processing is finished, you are ready to analyze the output:



```
ControlSet001\Control\Session Manager\AppCertDlls not found.
----------------------------------------
appcompatcache v.20160528
(System) Parse files from System hive AppCompatCache

ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: Fri Mar 10 11:31:40 2017 Z
Signature: 0xbadc0fee
Win2K8R2/Win7, 32-bit
C:\Windows\Installer\MSI6CF8.tmp  Wed Nov 12 10:31:44 2014 Z  Executed
C:\Windows\System32\sdclt.exe  Sat Nov 20 01:17:38 2010 Z  Executed
C:\Windows\System32\syncui.dll  Sat Nov 20 01:21:28 2010 Z
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regtlibv12.exe  Fri Apr 11 20:08:06 2014 Z  Executed
C:\Program Files\Common Files\Doctor Web\Scanning Engine\dwwatcher.exe  Mon Nov  7 10:29:55 2016 Z  Executed
C:\Program Files\Windows Media Player\WMPNSSUI.dll  Tue Jul 14 01:16:19 2009 Z
C:\Windows\system32\lsass.exe  Tue Nov 11 15:05:11 2014 Z  Executed
E:\Activate Warranty.exe  Wed Sep 25 21:00:00 2013 Z
C:\Windows\system32\migwiz\postmig.exe  Tue Jul 14 01:14:24 2009 Z
D:\Service Pack 2 for Microsoft Office 2010 (KB2687455)\officesp2010-kb2687455-fullfile-x86-ru-ru.exe  Wed Nov 12 10:12:24 2014 Z  Executed
C:\Windows\Installer\MSI953F.tmp  Wed Nov 12 09:41:10 2014 Z  Executed
C:\Windows\System32\offfilt.dll  Tue Jul 14 01:16:12 2009 Z
C:\Windows\system32\net.exe  Tue Jul 14 01:14:27 2009 Z  Executed
C:\Program Files\Windows Mail\WinMail.exe  Tue Jul 14 01:14:45 2009 Z  Executed
C:\Windows\System32\appwiz.cpl  Sat Nov 20 01:16:52 2010 Z
C:\Program Files\Kyocera\ClientTool\KMSCN\KMSCNEML.exe  Sat Nov 10 01:29:37 2012 Z  Executed
D:\UpdatePack7R2-14.10.20.exe  Fri Nov  7 08:27:55 2014 Z
C:\Windows\system32\wuauclt.exe  Wed May 14 16:23:40 2014 Z  Executed
D:\867e2503d8f5914a3630517668a661\Setup.exe  Wed Sep  3 09:49:59 2014 Z  Executed
C:\Program Files\Common Files\Microsoft Shared\OFFICE14\MSOXMLED.EXE  Wed Oct 31 09:21:48 2012 Z  Executed
C:\Windows\system32\wevtutil.exe  Tue Jul 14 01:14:44 2009 Z  Executed
C:\Program Files\Unlocker\UnlockerCOM.dll  Sun Jul  4 21:32:37 2010 Z
```

Figure 6.10. RegRipper output

If you scroll down the output file, you will see that there is a lot of important information from a forensic point of view, such as connected USB devices, EventLog configuration, mounted devices, network connections, and so on. The tools work very fast, so this is a good tool set to start with.

How it works...

RegRipper uses Perl modules, according to the profile chosen by a forensic examiner, to extract data from a hive (registry) file, and save the output to a `TXT` file.

See also

The RegRipper download page:

`https://github.com/keydet89/RegRipper2.8`

Recovering deleted Registry artifacts with Registry Explorer

Registry Explorer is another free Windows Registry forensic tool by another famous digital forensic examiner: Eric Zimmerman. One of the extremely useful features of this tool is its capability to recover deleted records. And it's easier than you might imagine.

Getting ready

Go to Eric's GitHub and click on the Registry Explorer download link. In our case, it's called **Registry Explorer/RECmd Version 0.8.1.0**. As at the time of writing, the most recent version of the tool is 0.8.1.0. Once **RegistryExplorer_RECmd.zip** is downloaded, unpack it and you are ready to go.

How to do it...

The steps to recover deleted registry artifacts using registry explorer are as follows:

1. Start **RegistryExplorer.exe**, go to **Options** and make sure the **Recover deleted keys/values** option is enabled, as in the following figure:

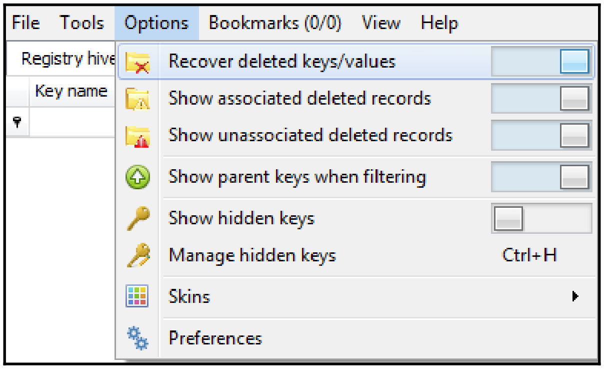
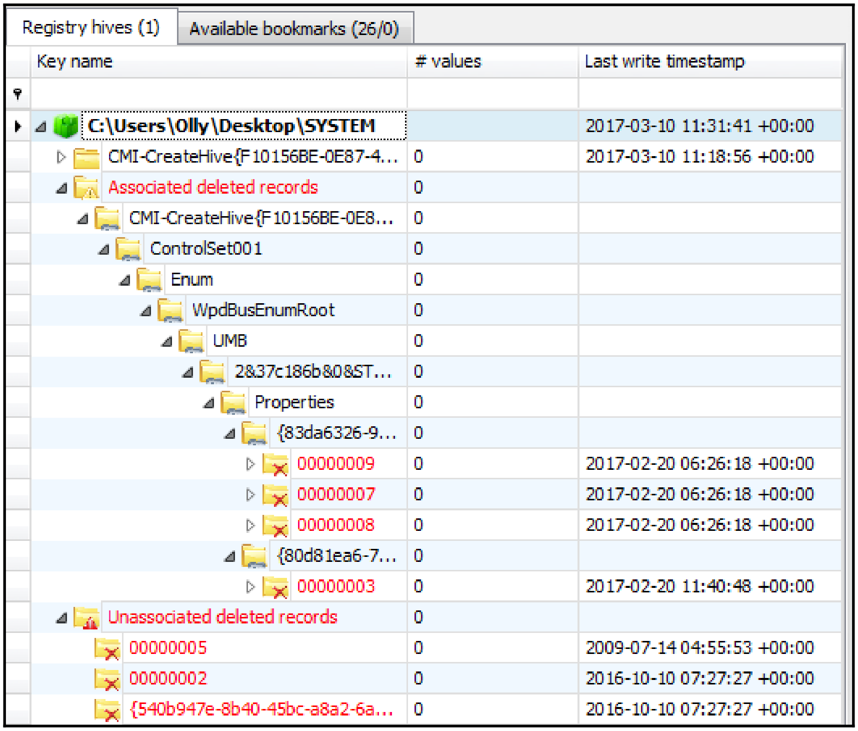

File
Tools
Options
Bookmarks (0/0)
View
Help
Registry hive
Key name
Recover deleted keys/values
Show associated deleted records
Show unassociated deleted records
Show parent keys when filtering
Show hidden keys
Manage hidden keys
Ctrl+H
Skins
Preferences

Figure 6.11. Registry Explorer Recover deleted keys/values option

Now you are ready to choose a hive file for processing. To do this, go to **File - Load offline hive**, or just press **Alt + 1**. That's it.

2. Now you can browse the contents of your hive file, in our case SYSTEM, including associated and unassociated deleted records, as you can see in the following figure:



Key name	# values	Last write timestamp
C:\Users\Olly\Desktop\SYSTEM		2017-03-10 11:31:41 +00:00
CMI-CreateHive{F10156BE-0E87-4...	0	2017-03-10 11:18:56 +00:00
Associated deleted records	0	
CMI-CreateHive{F10156BE-0E8...	0	
ControlSet001	0	
Enum	0	
WpdBusEnumRoot	0	
UMB	0	
2&37c186b&0&ST...	0	
Properties	0	
{83da6326-9...	0	
00000009	0	2017-02-20 06:26:18 +00:00
00000007	0	2017-02-20 06:26:18 +00:00
00000008	0	2017-02-20 06:26:18 +00:00
{80d81ea6-7...	0	
00000003	0	2017-02-20 11:40:48 +00:00
Unassociated deleted records	0	
00000005	0	2009-07-14 04:55:53 +00:00
00000002	0	2016-10-10 07:27:27 +00:00
{540b947e-8b40-45bc-a8a2-6a...	0	2016-10-10 07:27:27 +00:00

Figure 6.12. Associated and unassociated deleted records

The difference between associated and unassociated records is that the first group is still associated with keys in the active registry, and the second group is not.

How it works...

Registry Explorer processes the hive file of choice and automatically recovers deleted records, both associated and unassociated. Once processing is finished, an examiner can browse available data.

See also

Eric Zimmerman's GitHub:
`https://ericzimmerman.github.io/`

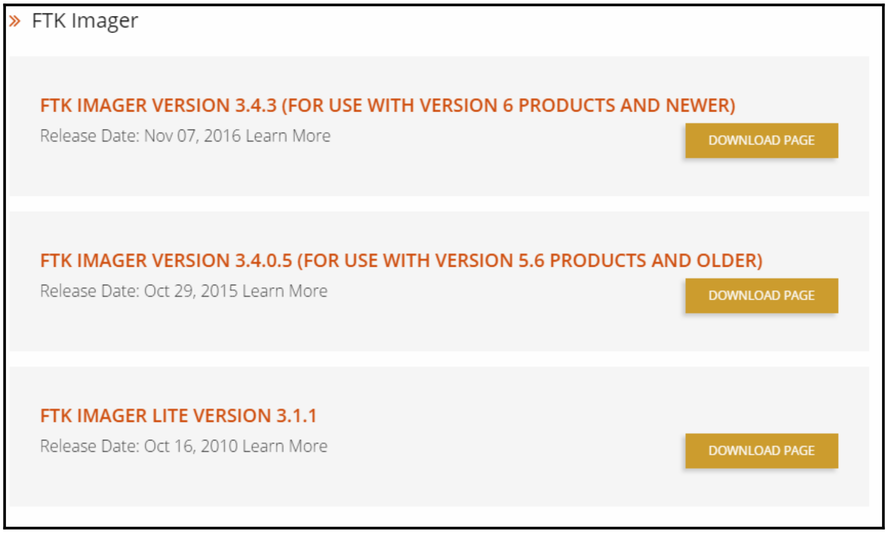
Introducing Registry Explorer:
`https://binaryforay.blogspot.ru/2015/02/introducing-registry-explorer.html`

Registry analysis with FTK Registry Viewer

FTK Registry Viewer ships as part of AccessData’s products, or can also be downloaded separately. It allows users to view the contents of the registry on a Windows machine.

Getting ready

If you already have FTK, Registry Viewer will be on your system. If you do not, you can download FTK Imager at AccessData’s website - it's free. You will need to fill in some personal information, including your name, company name, position and email address to gain access to the free download. The following figure shows the download page for FTK Imager:



» FTK Imager

FTK IMAGER VERSION 3.4.3 (FOR USE WITH VERSION 6 PRODUCTS AND NEWER)
Release Date: Nov 07, 2016 Learn More

FTK IMAGER VERSION 3.4.0.5 (FOR USE WITH VERSION 5.6 PRODUCTS AND OLDER)
Release Date: Oct 29, 2015 Learn More

FTK IMAGER LITE VERSION 3.1.1
Release Date: Oct 16, 2010 Learn More

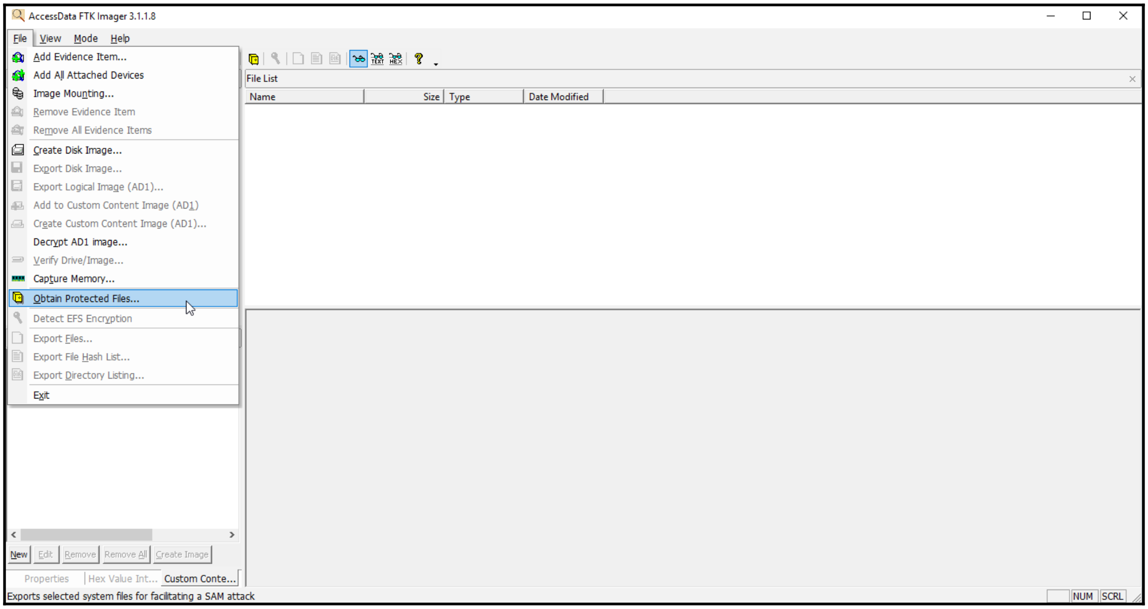
Figure 6.13. Downloading FTK Imager

If you only need to download Registry Viewer, you can do that on the **Product Downloads** page as well.

How to do it...

Once Registry Viewer has been installed, navigate to it on your machine and double-click the icon to open the program. Open FTK Imager at the same time.

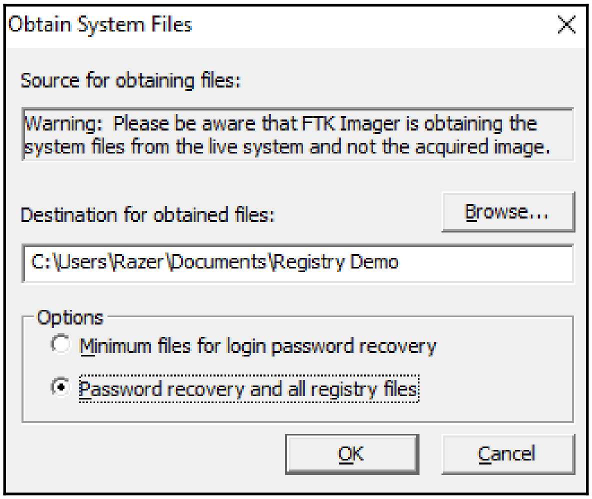
1. In Imager, go to **File** > **Obtain Protected Files**.



Exports selected system files for facilitating a SAM attack

Figure 6.14. Obtaining protected files

2. In the small box that pops up, choose a destination folder for your files.



Obtain System Files

Source for obtaining files:

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files:

C:\Users\Razer\Documents\Registry Demo

Options

○ Minimum files for login password recovery

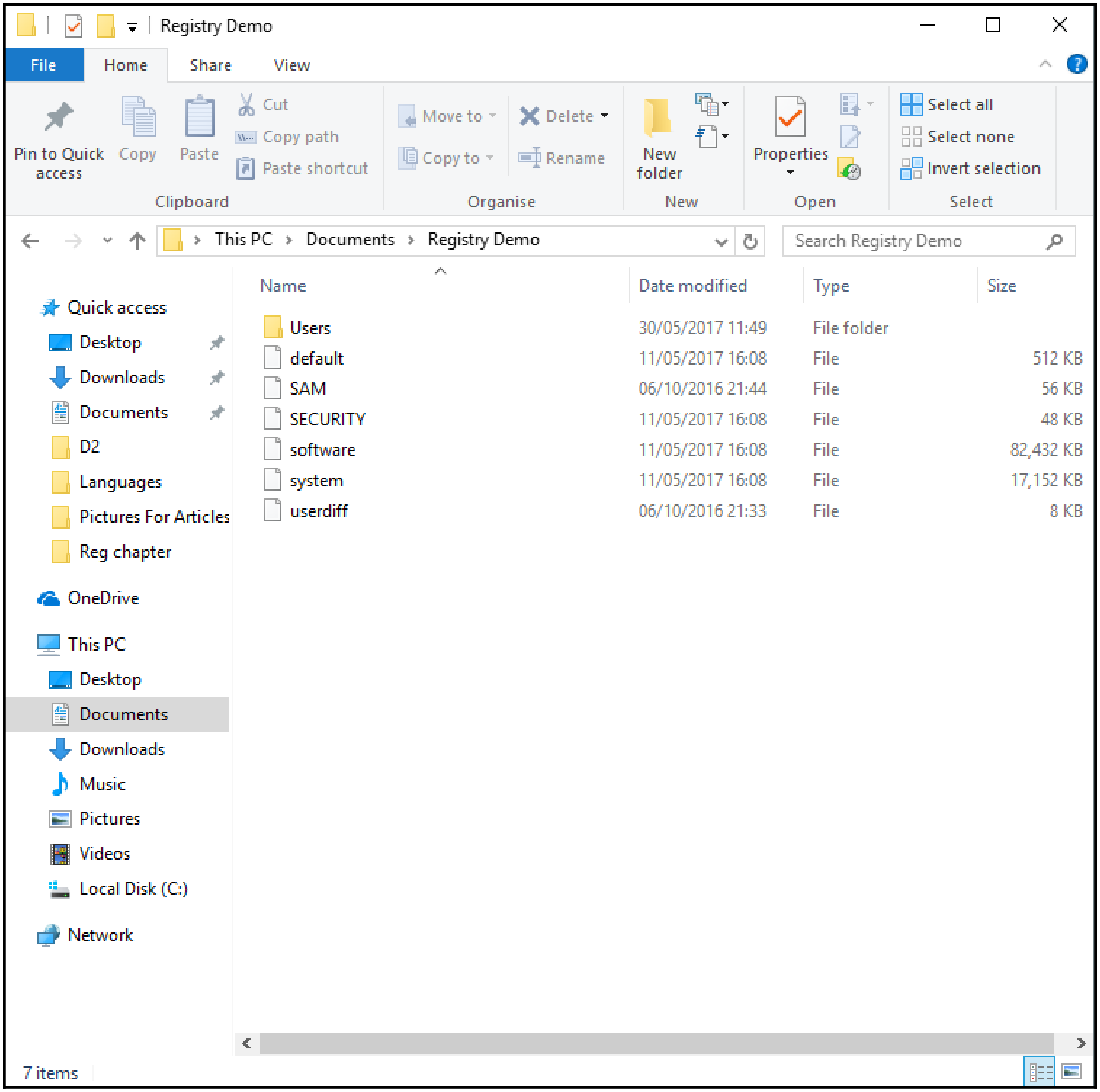
● Password recovery and all registry files

Figure 6.15. Choosing a destination folder

Note the warning about Imager getting the files from your own system. This is fine in an example like this, or as part of a practice case, but if it shows up when you're trying to find evidence on a forensic image, you know you've chosen the wrong source!

3. Make sure you choose **Password recovery and all registry files** from below the destination folder bar, otherwise you will only get a stripped-back version of the results. Click **OK**.

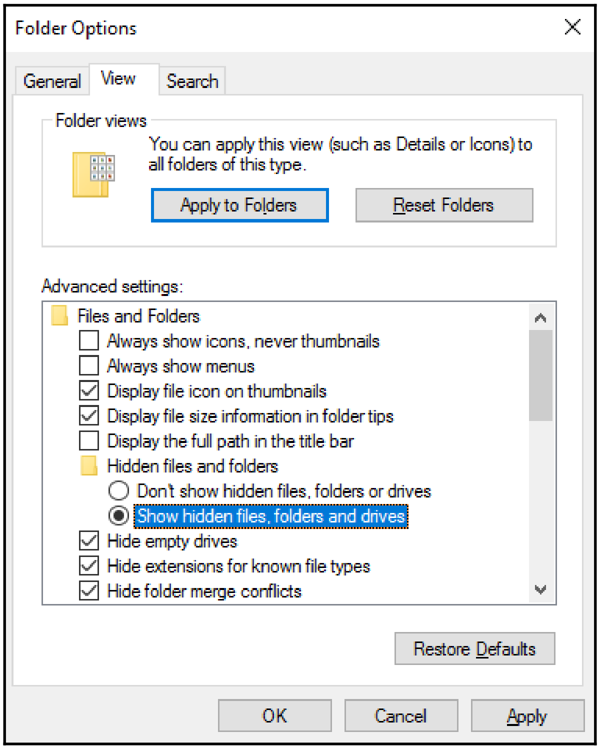
   It may take a little while to generate, and for the first few seconds it might look like nothing is happening. Remember, patience is a virtue when dealing with technology! You can check whether the process has finished by opening the folder in the file path you specified earlier, which should now be populated as shown in the following screenshot:



Name	Date modified	Type	Size
Users	30/05/2017 11:49	File folder	
default	11/05/2017 16:08	File	512 KB
SAM	06/10/2016 21:44	File	56 KB
SECURITY	11/05/2017 16:08	File	48 KB
software	11/05/2017 16:08	File	82,432 KB
system	11/05/2017 16:08	File	17,152 KB
userdiff	06/10/2016 21:33	File	8 KB

Figure 6.16. The populated folder

4. Click **File** and then **Change folder and Search Options**. This will open a dialogue box. Click the **View** tab and enable the option **Show hidden files, folders and drives** under **Hidden files and folders**.



You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

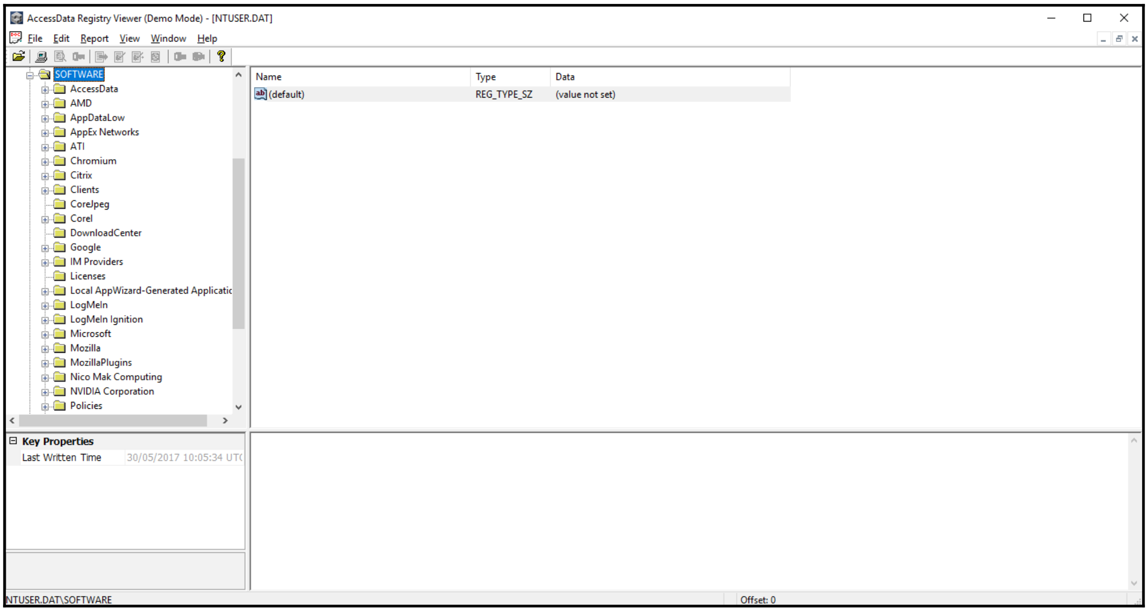
Files and Folders
- □ Always show icons, never thumbnails
- □ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- □ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders or drives
  - ● Show hidden files, folders and drives
- ☑ Hide empty drives
- ☑ Hide extensions for known file types
- ☑ Hide folder merge conflicts

Figure 6.17. Showing hidden files

Click **Apply** and then **OK**.

Now we can look at the data we have collected from the registry using Registry Viewer.

1. To do that, open Registry Viewer and click **File** > **Open**, then go to the folder in which you saved the registry files and find the one marked `NTUSER.DAT`. Open it.
2. The **SOFTWARE** menu will give you a nice long list of all the pieces of software that have been installed on the machine in question:

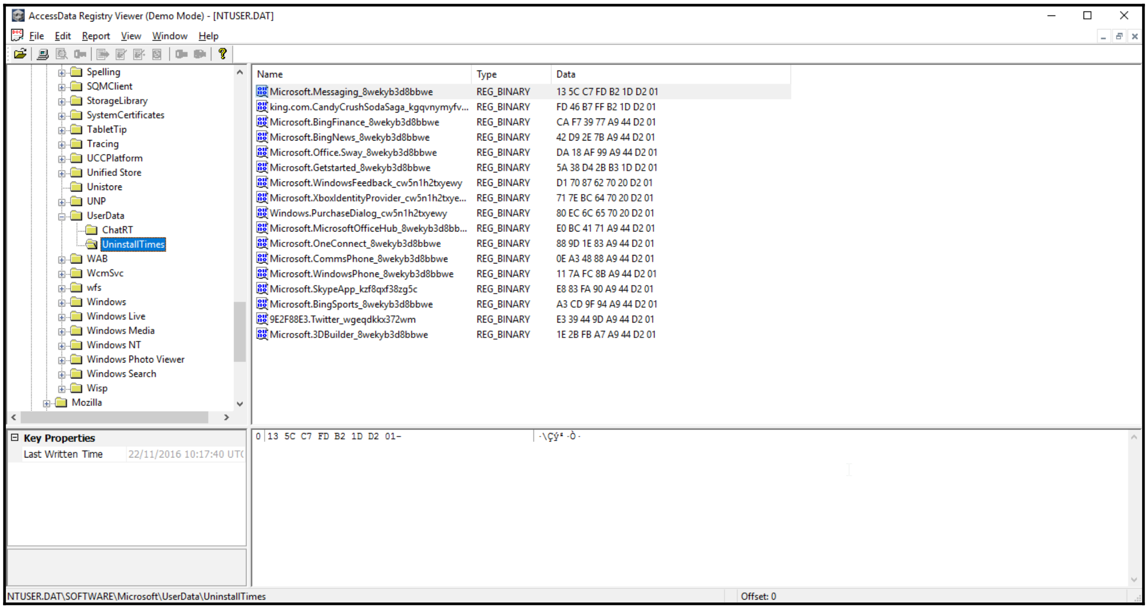


Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

Key Properties	
Last Written Time	30/05/2017 10:05:34 UT(

Figure 6.18. Software installed on the machine

3. You can see which programs have been uninstalled and when the uninstallations took place under `NTUSER.DAT\SOFTWARE\Microsoft\UserData\UninstallTimes`.



Name	Type	Data
Microsoft.Messaging_8wekyb3d8bbwe	REG_BINARY	13 5C C7 FD B2 1D D2 01
king.com.CandyCrushSodaSaga_kgqvnymyfv...	REG_BINARY	FD 46 B7 FF B2 1D D2 01
Microsoft.BingFinance_8wekyb3d8bbwe	REG_BINARY	CA F7 39 77 A9 44 D2 01
Microsoft.BingNews_8wekyb3d8bbwe	REG_BINARY	42 D9 2E 7B A9 44 D2 01
Microsoft.Office.Sway_8wekyb3d8bbwe	REG_BINARY	DA 18 AF 99 A9 44 D2 01
Microsoft.Getstarted_8wekyb3d8bbwe	REG_BINARY	5A 38 D4 2B B3 1D D2 01
Microsoft.WindowsFeedback_cw5n1h2txyewy	REG_BINARY	D1 70 87 62 70 20 D2 01
Microsoft.XboxIdentityProvider_cw5n1h2txye...	REG_BINARY	71 7E BC 64 70 20 D2 01
Windows.PurchaseDialog_cw5n1h2txyewy	REG_BINARY	80 EC 6C 65 70 20 D2 01
Microsoft.MicrosoftOfficeHub_8wekyb3d8bb...	REG_BINARY	E0 BC 41 71 A9 44 D2 01
Microsoft.OneConnect_8wekyb3d8bbwe	REG_BINARY	88 9D 1E 83 A9 44 D2 01
Microsoft.CommsPhone_8wekyb3d8bbwe	REG_BINARY	0E A3 48 88 A9 44 D2 01
Microsoft.WindowsPhone_8wekyb3d8bbwe	REG_BINARY	11 7A FC 8B A9 44 D2 01
Microsoft.SkypeApp_kzf8qxf38zg5c	REG_BINARY	E8 83 FA 90 A9 44 D2 01
Microsoft.BingSports_8wekyb3d8bbwe	REG_BINARY	A3 CD 9F 94 A9 44 D2 01
9E2F88E3.Twitter_wgeqdkkx372wm	REG_BINARY	E3 39 44 9D A9 44 D2 01
Microsoft.3DBuilder_8wekyb3d8bbwe	REG_BINARY	1E 2B FB A7 A9 44 D2 01

Key Properties

Last Written Time	22/11/2016 10:17:40 UT(

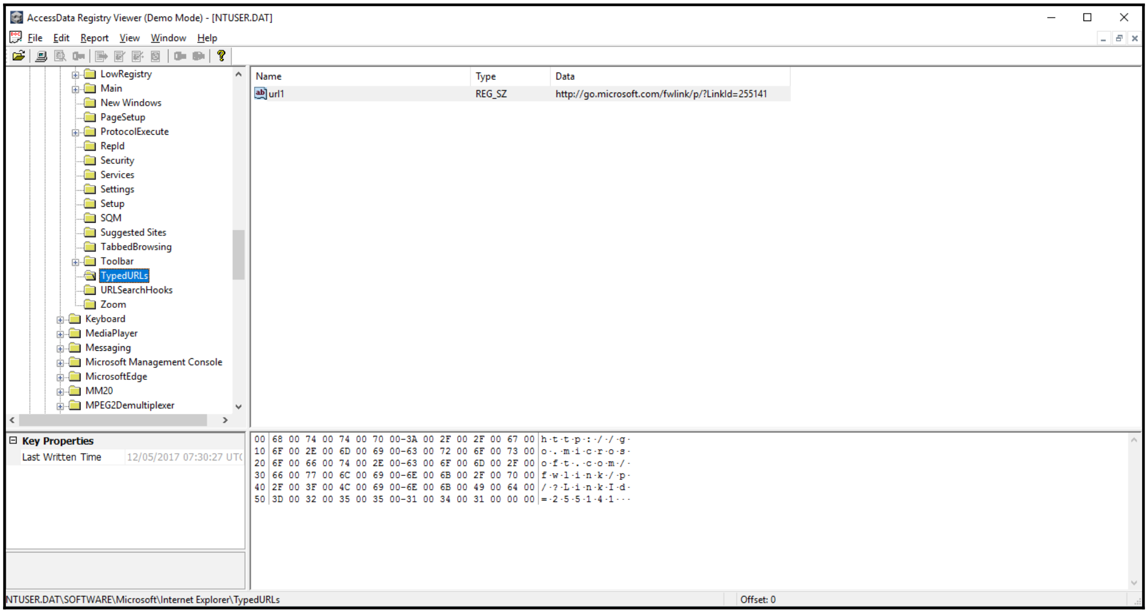
```
0 13 5C C7 FD B2 1D D2 01-
```

NTUSER.DAT\SOFTWARE\Microsoft\UserData\UninstallTimes   Offset: 0

Figure 6.19. Uninstall times

This can be particularly useful if you suspect that a user has been taking anti-forensic measures to try to scupper an investigation.

4. Under `NTUSER.DAT\SOFTWARE\Microsoft\InternetExplorer\TypedURLs`, you can see the addresses of any sites a user visited in Internet Explorer:



Name	Type	Data
url1	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

Last Written Time 12/05/2017 07:30:27 UTC

```
00 68 00 74 00 74 00 70 00-3A 00 2F 00 2F 00 67 00 h·t·t·p·:·/·/·g·
10 6F 00 2E 00 6D 00 69 00-63 00 72 00 6F 00 73 00 o·.·m·i·c·r·o·s·
20 6F 00 66 00 74 00 2E 00-63 00 6F 00 6D 00 2F 00 o·f·t·.·c·o·m·/·
30 66 00 77 00 6C 00 69 00-6E 00 6B 00 2F 00 70 00 f·w·l·i·n·k·/·p·
40 2F 00 3F 00 4C 00 69 00-6E 00 6B 00 49 00 64 00 /·?·L·i·n·k·I·d·
50 3D 00 32 00 35 00 35 00-31 00 34 00 31 00 00 00 =·2·5·5·1·4·1···
```

NTUSER.DAT\SOFTWARE\Microsoft\Internet Explorer\TypedURLs

Figure 6.20. Sites visited in Internet Explorer

Under **NTUSER.DAT\Software\Microsoft\Internet Explorer\IntelliForms**, you can see data from autocomplete forms, such as usernames and passwords.

How it works...

Registry Viewer collects registry files from a machine or a forensic image, allowing manual examination with FTK or Imager.

See also

AccessData's Products page:
`http://accessdata.com/product-download`

The AccessData Registry Viewer User Guide:
`https://ad-pdf.s3.amazonaws.com/RegistryViewer_UG.pdf`

7

Main Windows Operating System Artifacts

In this chapter, we will cover the following recipes:

- Recycle bin content analysis with EnCase Forensic
- Recycle bin content analysis with Rifiuti2
- Recycle bin content analysis with Magnet AXIOM
- Event log analysis with FullEventLogView
- Event log analysis with Magnet AXIOM
- Event log recovery with EVTXtract
- LNK file analysis with EnCase Forensic
- LNK file analysis with LECmd
- LNK file analysis with Link Parser
- Prefetch file analysis with Magnet AXIOM
- Prefetch file parsing with PECmd
- Prefetch file recovery with Windows Prefetch Carver

Introduction

Some features of Windows operating systems produce a great number of valuable artifacts that can be further used as pieces of digital evidence. The most common sources of such artifacts are the Recycle Bin, Windows Event Logs, LNK files, and Prefetch files.

The Recycle Bin contains files and folders that have been deleted by the user via the right-click menu. In fact, these files are not deleted from the file system, but only moved from their original location into the Recycle Bin. There are two formats of the Recycle Bin: the Recycler format (Windows 2000, XP) - files are stored under `C:\Recycler\%SID%\` and their metadata is stored in the `INFO2` file; and the `$Recycle.Bin` format - files are stored under `C:\$Recycle.Bin\%SID%\` in `$R` file, and their metadata is stored in $I files.

As you can guess from the name, Windows Event Logs collect information about different system events. Windows 2000, XP, and 2003 (except for server versions) store these logs in three files: Application, System, and Security. These files can be found under `C:\Windows\system32\config`. With Windows Vista, the Event Logs format has been changed to XML. These EVTX files can be found under `C:\Windows\System32\Winevt\Logs`.

LNK files or Windows Shortcut files refer to other files: applications, documents, and so on. These can be found system-wide, and can help a digital forensic examiner to uncover some of the suspect's activities, including recently used files, applications, and so on.

And, finally, Prefetch files. You can find these files in `C:\Windows\Prefetch`, and they contain lots of valuable information about used applications, including their run count, last run date and time, and so on.

In this chapter, you will learn how to analyze all of these sources of digital evidence with both commercial and free digital forensics tools.

Recycle Bin content analysis with EnCase Forensic

EnCase is a well-known and court-accepted commercial digital forensics tool developed by Guidance Software. It is used by examiners from all over the world, both in law enforcement agencies and in the private sector. It supports the whole investigation life cycle, from collecting to reporting. What's more, it has a built-in scripting language - EnScript - so users can write their own scripts to solve digital forensic problems. A lot of useful EnScripts are available for free at EnCase App Central. In this recipe, we will show you how to use this powerful tool to examine Windows Recycle Bin contents.

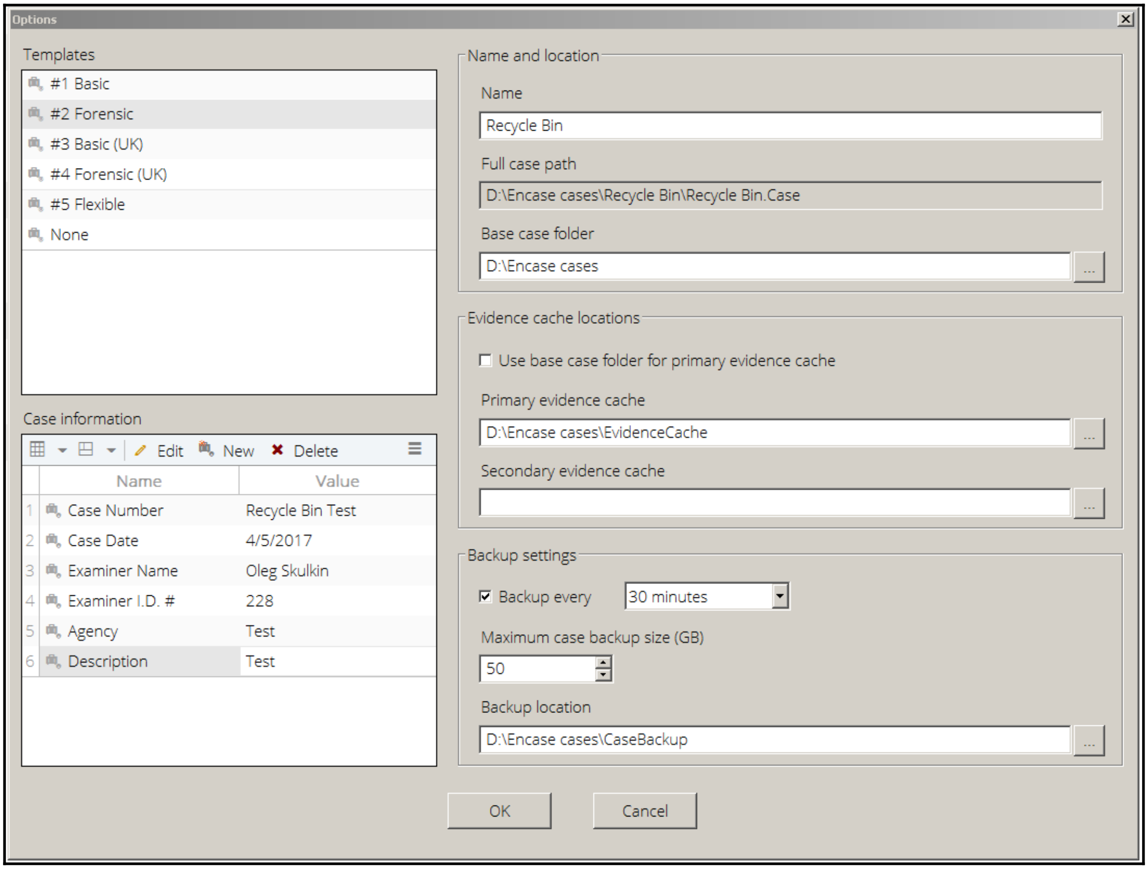
Getting ready

Unfortunately, Guidance Software doesn't provide trial versions of EnCase Forensic, so to follow this recipe, you must have a valid licence. If you have one, make sure you are using the latest version of the tool: EnCase Forensic 8.

How to do it...

The steps for Recycle bin Content Analysis in Encase Forensic are as follows:

1. Let's start by creating a new case. To do this, click on the **New Case** link on the left. The Case **Options** window will pop up, as you see in the following figure:



Options

Templates

- #1 Basic
- #2 Forensic
- #3 Basic (UK)
- #4 Forensic (UK)
- #5 Flexible
- None

Case information

	Name	Value
1	Case Number	Recycle Bin Test
2	Case Date	4/5/2017
3	Examiner Name	Oleg Skulkin
4	Examiner I.D. #	228
5	Agency	Test
6	Description	Test

Name and location

Name: Recycle Bin

Full case path: D:\Encase cases\Recycle Bin\Recycle Bin.Case

Base case folder: D:\Encase cases

Evidence cache locations

□ Use base case folder for primary evidence cache

Primary evidence cache: D:\Encase cases\EvidenceCache

Secondary evidence cache:

Backup settings

☑ Backup every 30 minutes

Maximum case backup size (GB): 50

Backup location: D:\Encase cases\CaseBackup

Figure 7.1. Case Options

2. We have chosen #**2 Forensic** template, and there is a lot of information to fill in. Let's start with Case information. Here, we have 6 fields to fill in: **Case Number**, **Case Data**, **Examiner Name**, **Examiner I.D.**, **Agency,** and **Description**. All fields are self-explanatory, so just fill them in.
3. Let's go to **Name and location**. Type your case's name or number in the first field, and choose the **Base case folder** (case files will be stored here). The **Full case path** field will be filled in automatically.
4. Go to **Evidence cache locations**. You can use the same folder to store cache (to do this, tick **Use base case folder for primary evidence cache**), or choose one or two folders to store it.
5. Finally, if you want your case to be backed up, tick the **Backup every** option and choose its value. Don't forget about choosing the backup folder and the maximum size of the backup. Once everything is filled in, just click **OK**.
6. Now you see a window with your case information, and you are ready to add a forensic image. To do this, click the **Add Evidence File** link on the left.

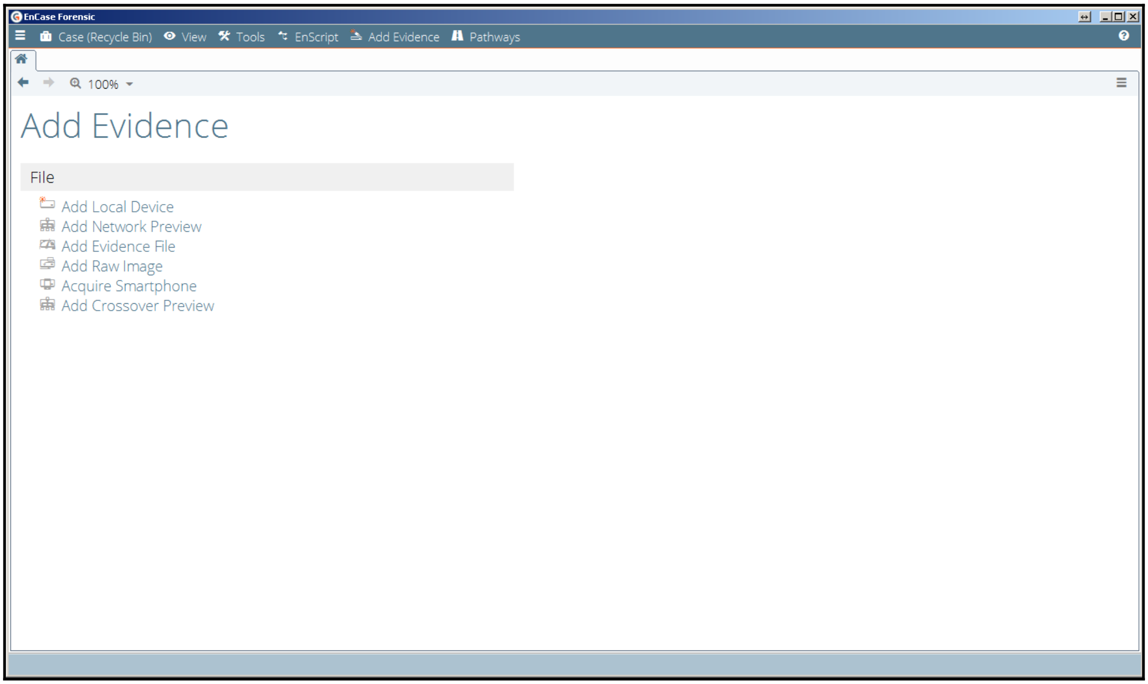
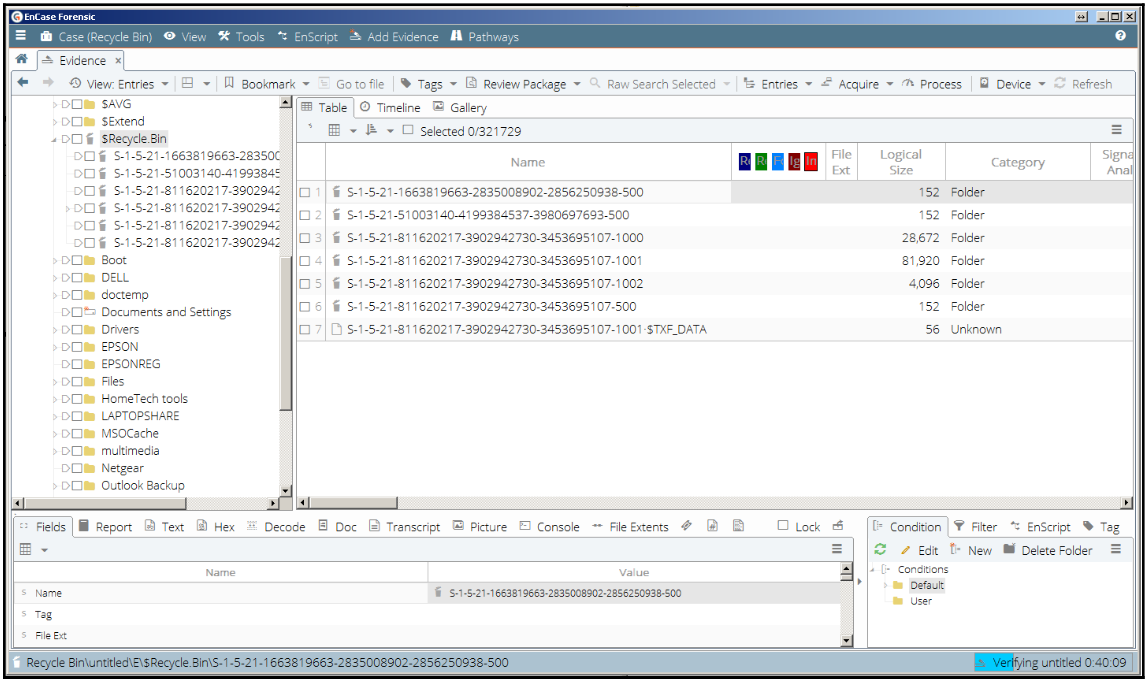


Figure 7.2. Adding evidence

As you can see in the preceding screenshot, there are 6 evidence source options: you can **Add Local Device** (don't forget to use a writeblocker), a remote evidence source, E01 or RAW image, and so on. You already have both, an E01 and a RAW image, so you can use one of them. We are going to use an E01 image. If you too, plan to use an E01 image, click the **Add Evidence File** link; if you are using a RAW image, click **Add Raw Image**.

7. Now you see your evidence file. Click on its name to see the contents. It may take some time for EnCase to parse the data. Once data parsing is finished, go to the **$Recycle bin** folder:



- $AVG
- $Extend
- $Recycle.Bin
  - S-1-5-21-1663819663-283500
  - S-1-5-21-51003140-41993845
  - S-1-5-21-811620217-3902942
  - S-1-5-21-811620217-3902942
  - S-1-5-21-811620217-3902942
  - S-1-5-21-811620217-3902942
- Boot
- DELL
- doctemp
- Documents and Settings
- Drivers
- EPSON
- EPSONREG
- Files
- HomeTech tools
- LAPTOPSHARE
- MSOCache
- multimedia
- Netgear
- Outlook Backup

Selected 0/321729

	Name	Rı Rı Fı Ig In	File Ext	Logical Size	Category	Signa Anal
☐ 1	S-1-5-21-1663819663-2835008902-2856250938-500			152	Folder	
☐ 2	S-1-5-21-51003140-4199384537-3980697693-500			152	Folder	
☐ 3	S-1-5-21-811620217-3902942730-3453695107-1000			28,672	Folder	
☐ 4	S-1-5-21-811620217-3902942730-3453695107-1001			81,920	Folder	
☐ 5	S-1-5-21-811620217-3902942730-3453695107-1002			4,096	Folder	
☐ 6	S-1-5-21-811620217-3902942730-3453695107-500			152	Folder	
☐ 7	S-1-5-21-811620217-3902942730-3453695107-1001·$TXF_DATA			56	Unknown	

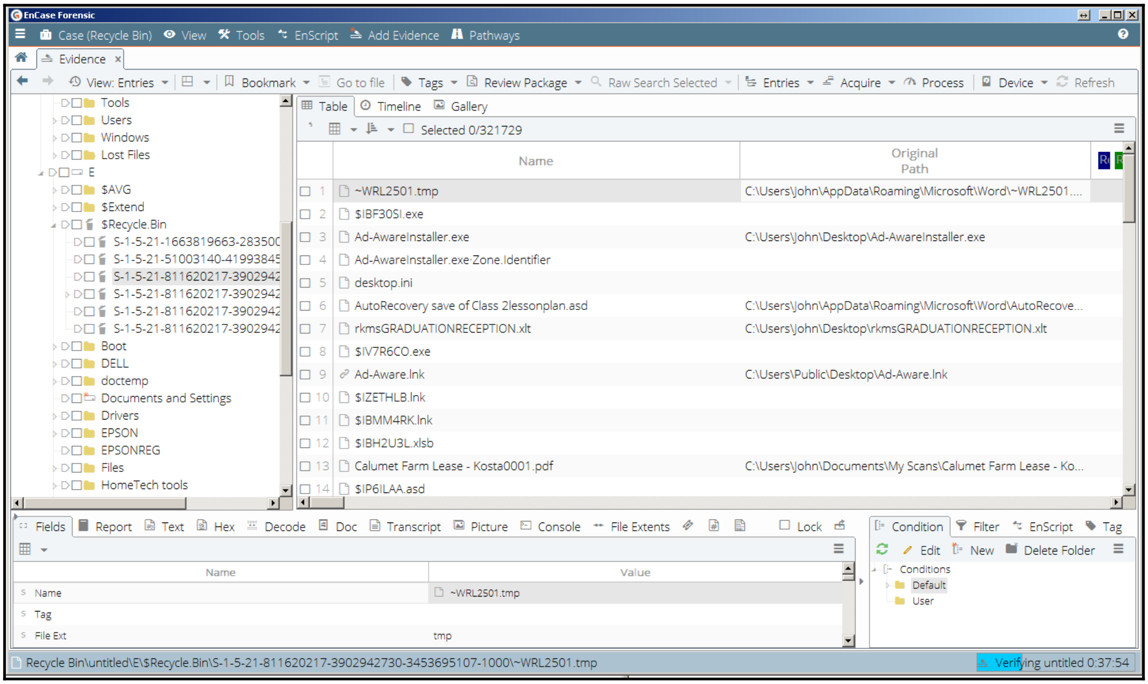
Name	Value
Name	S-1-5-21-1663819663-2835008902-2856250938-500
Tag	
File Ext	

Recycle Bin\untitled\E\$Recycle.Bin\S-1-5-21-1663819663-2835008902-2856250938-500

Verifying untitled 0:40:09

Figure 7.3. $Recycle.Bin folder contents

As you can see in the preceding figure, there is a list of the user's security identifiers (SID). This can help an examiner to determine which user placed files into the recycle bin. There are folders too; let's open one of them. In our case, we open the folder `S-1-5-21-811620217-3902942730-3453695107-1000`. Look at the next figure:



	Name	Original Path
1	~WRL2501.tmp	C:\Users\John\AppData\Roaming\Microsoft\Word\~WRL2501....
2	$IBF30SI.exe	
3	Ad-AwareInstaller.exe	C:\Users\John\Desktop\Ad-AwareInstaller.exe
4	Ad-AwareInstaller.exe·Zone.Identifier	
5	desktop.ini	
6	AutoRecovery save of Class 2lessonplan.asd	C:\Users\John\AppData\Roaming\Microsoft\Word\AutoRecove...
7	rkmsGRADUATIONRECEPTION.xlt	C:\Users\John\Desktop\rkmsGRADUATIONRECEPTION.xlt
8	$IV7R6CO.exe	
9	Ad-Aware.lnk	C:\Users\Public\Desktop\Ad-Aware.lnk
10	$IZETHLB.lnk	
11	$IBMM4RK.lnk	
12	$IBH2U3L.xlsb	
13	Calumet Farm Lease - Kosta0001.pdf	C:\Users\John\Documents\My Scans\Calumet Farm Lease - Ko...
14	$IP6ILAA.asd	

Name	Value
Name	~WRL2501.tmp
Tag	
File Ext	tmp

Recycle Bin\untitled\E\$Recycle.Bin\S-1-5-21-811620217-3902942730-3453695107-1000\~WRL2501.tmp

Figure 7.4. S-1-5-21-811620217-3902942730-3453695107-1000 folder contents

EnCase has parsed the Recycle Bin contents for you automatically. Also, it has gathered a lot of valuable information: the original file name, its original path, deletion date and time, and so on.

How it works...

Depending on the Windows version, EnCase extracts information about the Recycle Bin contents from an `INFO2` file (Windows XP) or `$I` and `$R` files (Windows Vista and above), so a forensic examiner can preview them and see their original names, path, deletion dates, and so on.

See also

What's New in EnCase Forensic 8:
`https://www.guidancesoftware.com/document/product-brief/what's-new-in-encase-forensic-8`

Recycle bin content analysis with Rifiuti2

Rifiuti2 is an open source tool which enables a computer forensic examiner to analyze Windows recycle bin content. The tool will show you important information such as the recycled file's deletion date and time, its original path, and so on. Rifiuti2 supports both old (starting from Windows 95) and modern (up to Windows 10) recycle bin formats. What's more, language is no problem: the tool supports all localized versions of Windows.

Getting ready

Go to Rifiuti2's download page and download the ZIP archive with the latest Windows version. In our case, the latest version is 0.6.1, so the archive we downloaded, is called **Rifiuti2-0.6.1-win.zip**. Unpack it and you are ready to go.

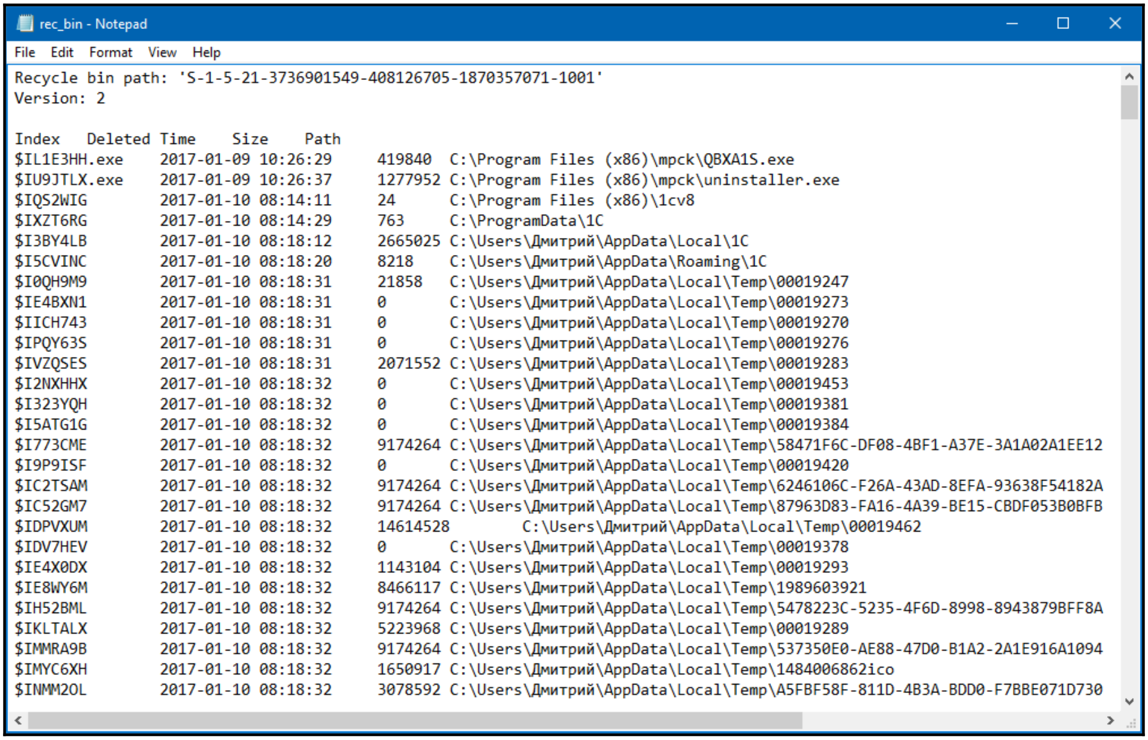
How to do it...

You already know that each user has their own folder in the recycle bin. Remember, the screenshot from the previous recipe about EnCase —there were a number of folders. To use Rifiuti2, you should first export one of those folders. There are a lot of tools capable of doing this, and you already know some of them, for example Autopsy, FTK Imager, and Magnet AXIOM.

Once you have exported the folder, you are ready to start the Windows Command Prompt and use the tool. If you are using a 32-bit system, go to the x32 folder; if you have a 64-bit system, go to the x64 folder. In both folders, you will find two Windows executables: `rifiuti.exe` and `rifiuti-vista.exe`. If you exported your folder from a Windows system up to (and including) XP, use `rifiuti.exe`, otherwise (starting from Vista) use `rifiuti-vista.exe`. In our case, the folder was exported from a Windows 10 image, so we used `rifiuti-vista.exe`.

```
rifiuti-vista.exe S-1-5-21-3736901549-408126705-1870357071-1001 >
rec_bin.txt
```

As you can see, we redirected the output to a TXT file. Look at its contents in the following figure :



```
Recycle bin path: 'S-1-5-21-3736901549-408126705-1870357071-1001'
Version: 2

Index   Deleted Time    Size    Path
$IL1E3HH.exe    2017-01-09 10:26:29     419840  C:\Program Files (x86)\mpck\QBXA1S.exe
$IU9JTLX.exe    2017-01-09 10:26:37     1277952 C:\Program Files (x86)\mpck\uninstaller.exe
$IQS2WIG        2017-01-10 08:14:11     24      C:\Program Files (x86)\1cv8
$IXZT6RG        2017-01-10 08:14:29     763     C:\ProgramData\1C
$I3BY4LB        2017-01-10 08:18:12     2665025 C:\Users\Дмитрий\AppData\Local\1C
$I5CVINC        2017-01-10 08:18:20     8218    C:\Users\Дмитрий\AppData\Roaming\1C
$I0QH9M9        2017-01-10 08:18:31     21858   C:\Users\Дмитрий\AppData\Local\Temp\00019247
$IE4BXN1        2017-01-10 08:18:31     0       C:\Users\Дмитрий\AppData\Local\Temp\00019273
$IICH743        2017-01-10 08:18:31     0       C:\Users\Дмитрий\AppData\Local\Temp\00019270
$IPQY63S        2017-01-10 08:18:31     0       C:\Users\Дмитрий\AppData\Local\Temp\00019276
$IVZQSES        2017-01-10 08:18:31     2071552 C:\Users\Дмитрий\AppData\Local\Temp\00019283
$I2NXHHX        2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019453
$I323YQH        2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019381
$I5ATG1G        2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019384
$I773CME        2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\58471F6C-DF08-4BF1-A37E-3A1A02A1EE12
$I9P9ISF        2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019420
$IC2TSAM        2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\6246106C-F26A-43AD-8EFA-93638F54182A
$IC52GM7        2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\87963D83-FA16-4A39-BE15-CBDF053B0BFB
$IDPVXUM        2017-01-10 08:18:32     14614528        C:\Users\Дмитрий\AppData\Local\Temp\00019462
$IDV7HEV        2017-01-10 08:18:32     0       C:\Users\Дмитрий\AppData\Local\Temp\00019378
$IE4X0DX        2017-01-10 08:18:32     1143104 C:\Users\Дмитрий\AppData\Local\Temp\00019293
$IE8WY6M        2017-01-10 08:18:32     8466117 C:\Users\Дмитрий\AppData\Local\Temp\1989603921
$IH52BML        2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\5478223C-5235-4F6D-8998-8943879BFF8A
$IKLTALX        2017-01-10 08:18:32     5223968 C:\Users\Дмитрий\AppData\Local\Temp\00019289
$IMMRA9B        2017-01-10 08:18:32     9174264 C:\Users\Дмитрий\AppData\Local\Temp\537350E0-AE88-47D0-B1A2-2A1E916A1094
$IMYC6XH        2017-01-10 08:18:32     1650917 C:\Users\Дмитрий\AppData\Local\Temp\1484006862ico
$INMM2OL        2017-01-10 08:18:32     3078592 C:\Users\Дмитрий\AppData\Local\Temp\A5FBF58F-811D-4B3A-BDD0-F7BBE071D730
```

Figure 7.5. Rifiuti2 output

Everything is parsed correctly. We have original paths, names, sizes, and deletion timestamps. Have you noticed the Cyrillic symbols? As we mentioned before, all localized versions of Windows are supported!

How it works...

If you have a folder from a Windows system prior to Vista, you can use `rifiuti.exe`, which parses `INFO2` file contents and extracts information about the particular user's recycle bin contents.

If you have a folder from a Windows Vista system or later, you use `rifiuti-vista.exe`, which parses the so-called index files ($I) to extract information about recycled files, their original paths, names, sizes, and deletion dates and times.

See also

Rifiuti2 GitHub page:
`https://github.com/abelcheung/rifiuti2`

Rifiuti2, ver. 0.6.1, download page:
`https://github.com/abelcheung/rifiuti2/releases/tag/0.6.1`

Recycle bin content analysis with Magnet AXIOM

Magnet AXIOM supports all common Windows operating system artifacts including, of course, the Recycle Bin. In this recipe, we will show you how to use it to analyze files which our suspect has tried to delete, putting them into the Recycle Bin.

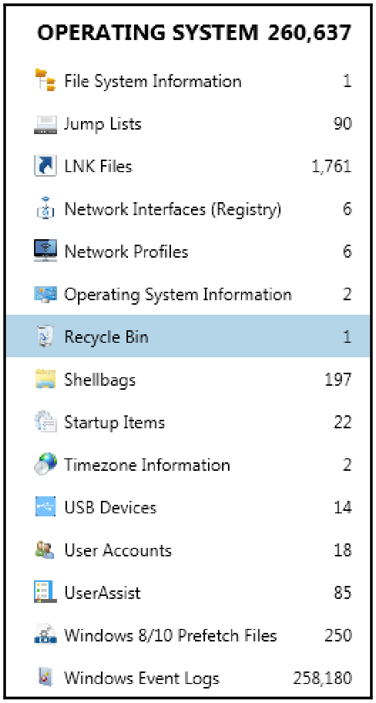
Getting ready

If you haven't downloaded and installed the trial version of Magnet AXIOM yet, use the link from the *See more* section to do so. Once the tool is installed on your workstation, open it, create a new case, add a forensic image, and process it with default options. If you don't know how to do this, refer back to the recipes in the previous chapters.

How to do it...

The steps for Recycle bin content analysis with magnet AXIOM are as follows:

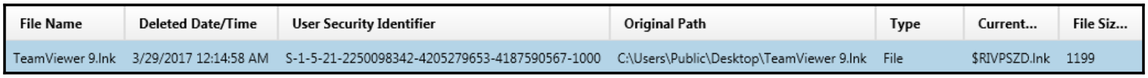
1. Once your forensic image is processed, go to AXIOM Examine's artifact types pane, and scroll down to **OPERATING SYSTEM**, as shown in the following figure:



OPERATING SYSTEM	260,637
File System Information	1
Jump Lists	90
LNK Files	1,761
Network Interfaces (Registry)	6
Network Profiles	6
Operating System Information	2
Recycle Bin	1
Shellbags	197
Startup Items	22
Timezone Information	2
USB Devices	14
User Accounts	18
UserAssist	85
Windows 8/10 Prefetch Files	250
Windows Event Logs	258,180

Figure 7.6. Operating system artifacts list

2. As you can see, there are quite a lot of different operating system artifacts listed, including the Recycle Bin. In our case, there is only one file there. You can see it in the following figure:



File Name	Deleted Date/Time	User Security Identifier	Original Path	Type	Current...	File Siz...
TeamViewer 9.lnk	3/29/2017 12:14:58 AM	S-1-5-21-2250098342-4205279653-4187590567-1000	C:\Users\Public\Desktop\TeamViewer 9.lnk	File	$RIVPSZD.lnk	1199

Figure 7.7. Recycle Bin contents

3. So, we have a link file for the TeamViewer app in our suspect's Recycle Bin. This app is used for remote access. Suspicious, isn't it? You can also find information about the date and time the file was deleted, the security identifier of the user who deleted it, and the original file path - everything you may need for your investigation.

How it works...

If you process the evidence source with the default options itself, or choose the Recycle Bin in your custom artifact list, Magnet AXIOM parses all available information from the `INFO2` file (up to Windows XP) or $I and $R files (starting from Windows Vista).

See also

Magnet AXIOM trial request page:

`https://www.magnetforensics.com/try-magnet-axiom-free-30-days/`

Event log analysis with FullEventLogView

FullEventLogView is another useful free tool from NirSoft, capable of parsing Windows 10, 8, 7, and Vista event logs. A computer forensic examiner can use it to view both event logs from a local computer and EVTX files, which can be found at `%SystemRoot%\Windows\System32\winevt\Logs`.

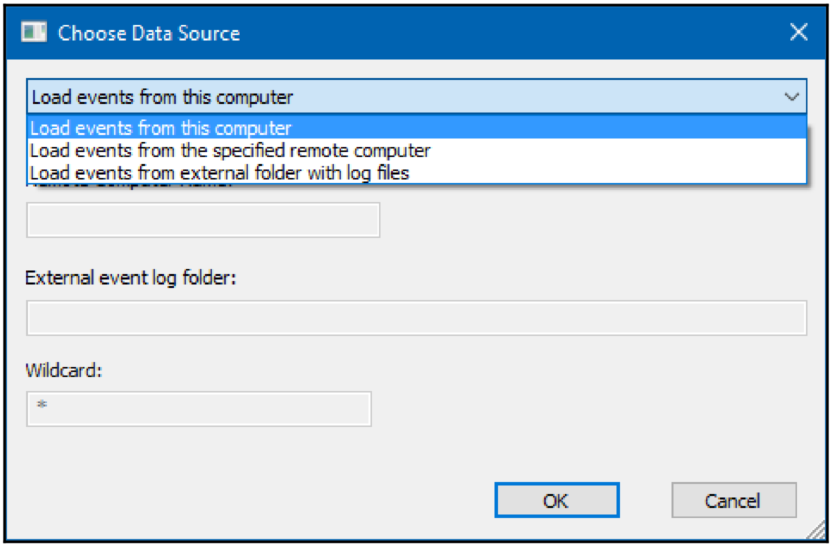
Getting ready

Go to the FullEventLogView download page on NirSoft's website (the link is presented in the See Also section), and get the 32-bit or 64-bit version of the tool, according to your system. Unpack the archive you downloaded and you are ready to go.

How to do it...

The steps for event log analysis with FullEventLogView are as follows:

1. The first thing you should do after starting the tool is choose the data source. To do this, go to **File** - **Choose Data Source,** or just press *F7*. As you can see in the following figure, there are three options available:
   - Loading logs from the computer you are running the tool on
   - Loading logs from a remote computer
   - Loading logs from a folder you previously exported (from a forensic image, for example)


Choose Data Source
Load events from this computer
Load events from this computer
Load events from the specified remote computer
Load events from external folder with log files
External event log folder:
OK
Cancel

Wildcard: *

Figure 7.8. Choosing data source in FullEventLogView

2. By default, **FullEventLogView** shows events only from the last 7 days. If you need a longer period, go to **Options** - **Advanced Options** (or press *F9*), and choose **Show events from all times**. You can also choose a time period to show, both in local time and GMT, and filter event logs by level, event ID, provider, and channel.

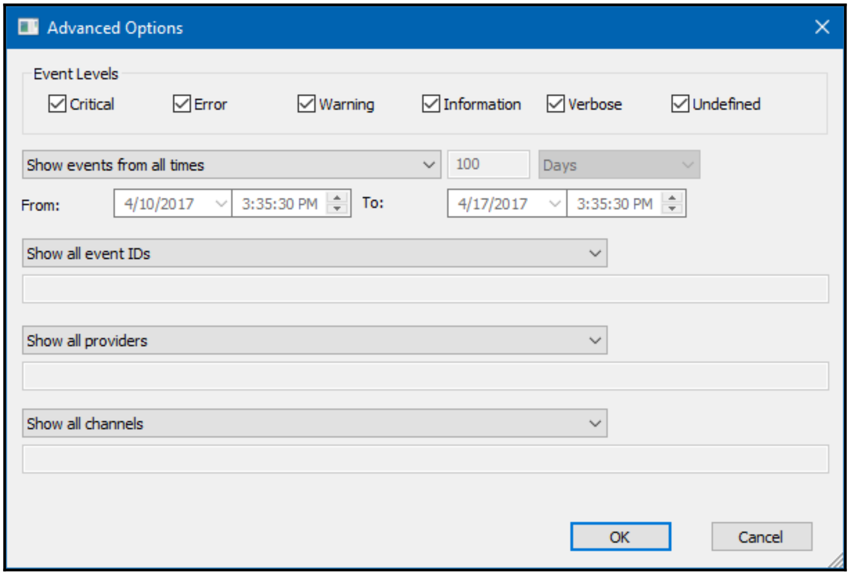
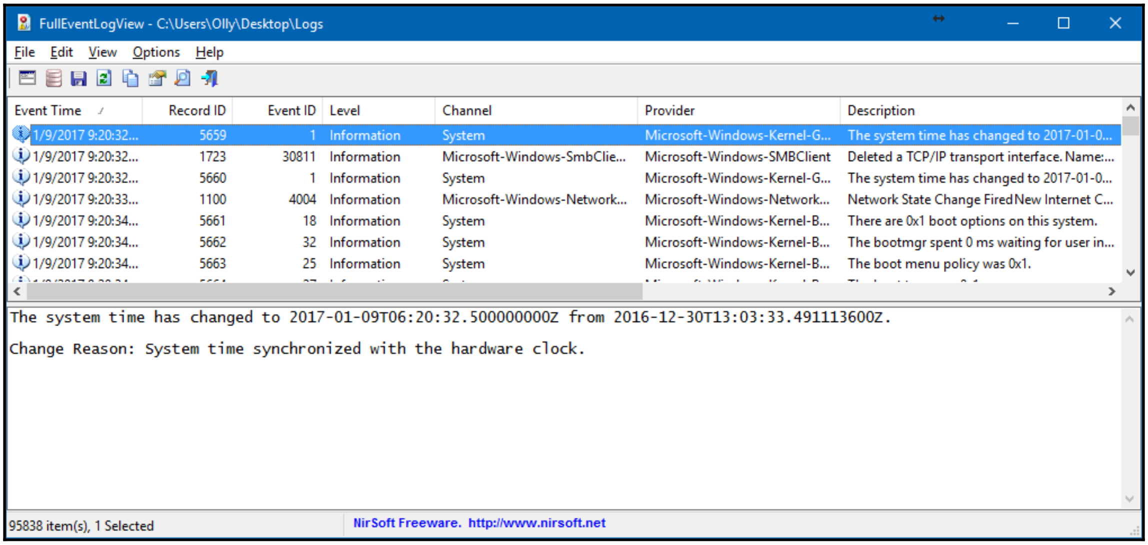


Figure 7.9. FullEventLogView Advanced Options

3. Once you have applied all the filters you need and chosen the data source, you will see all the available event logs in the main window of **FullEventLogView**. This is shown in the following figure:



Event Time	Record ID	Event ID	Level	Channel	Provider	Description
1/9/2017 9:20:32...	5659	1	Information	System	Microsoft-Windows-Kernel-G...	The system time has changed to 2017-01-0...
1/9/2017 9:20:32...	1723	30811	Information	Microsoft-Windows-SmbClie...	Microsoft-Windows-SMBClient	Deleted a TCP/IP transport interface. Name:...
1/9/2017 9:20:32...	5660	1	Information	System	Microsoft-Windows-Kernel-G...	The system time has changed to 2017-01-0...
1/9/2017 9:20:33...	1100	4004	Information	Microsoft-Windows-Network...	Microsoft-Windows-Network...	Network State Change FiredNew Internet C...
1/9/2017 9:20:34...	5661	18	Information	System	Microsoft-Windows-Kernel-B...	There are 0x1 boot options on this system.
1/9/2017 9:20:34...	5662	32	Information	System	Microsoft-Windows-Kernel-B...	The bootmgr spent 0 ms waiting for user in...
1/9/2017 9:20:34...	5663	25	Information	System	Microsoft-Windows-Kernel-B...	The boot menu policy was 0x1.

```
The system time has changed to 2017-01-09T06:20:32.500000000Z from 2016-12-30T13:03:33.491113600Z.

Change Reason: System time synchronized with the hardware clock.
```

95838 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Figure 7.10. Viewing event logs from a folder exported from an image

An examiner can sort the logs by any column available. Also, you can search through the logs: go to **Edit** - **Find**, or just press *Ctrl+F*.

How it works...

Depending on the data source, FullEventLogView displays event logs from the local computer, a remote computer, or a folder and enables digital forensic examiners to sort them and search through them using keywords.

See also

Event Logs:
`https://technet.microsoft.com/en-us/library/cc722404(v=ws.11).aspx`

FullEventLogView download page:
`http://www.nirsoft.net/utils/full_event_log_view.html`

Event log analysis with Magnet AXIOM

Let's keep using Magnet AXIOM to explore some of the most common Windows OS forensic artifacts. In this recipe, we will show you how to examine Windows Event Logs using this tool.

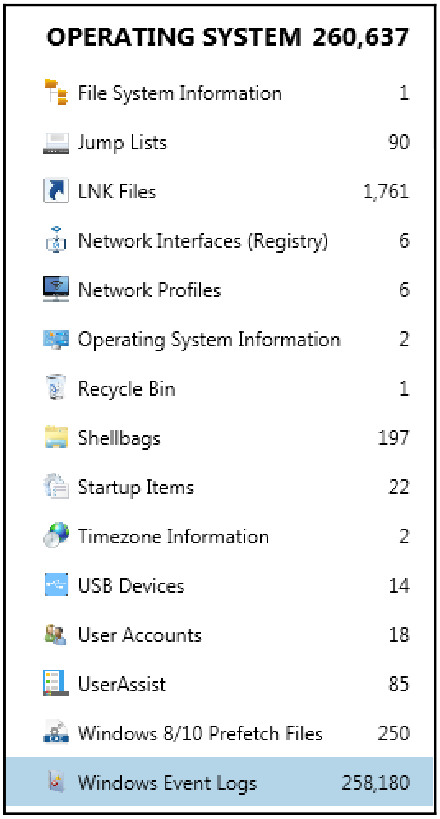
Getting ready

You have already used this tool recently to collect the Recycle Bin data from a forensic image. This time, we are interested in Event Logs examination, but you can use the same case as for the Recycle Bin if you processed the whole image with default options.

How to do it...

The steps for Event log analysis using Magnet AXIOM are as follows:

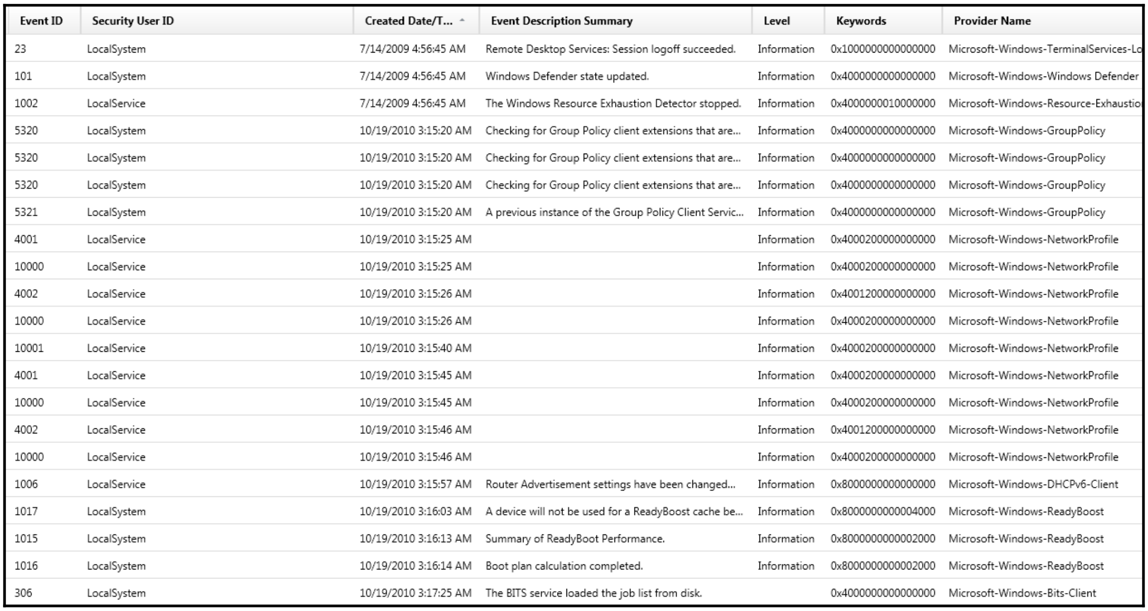
1. Open the case you used for the Recycle Bin forensic analysis and go to the OPERATING SYSTEM artifacts list again, but now choose **Windows Event Logs**, as in the following figure:



OPERATING SYSTEM	260,637
File System Information	1
Jump Lists	90
LNK Files	1,761
Network Interfaces (Registry)	6
Network Profiles	6
Operating System Information	2
Recycle Bin	1
Shellbags	197
Startup Items	22
Timezone Information	2
USB Devices	14
User Accounts	18
UserAssist	85
Windows 8/10 Prefetch Files	250
Windows Event Logs	258,180

Figure 7.11. Operating system artifacts list

2. As you can see in the preceding figure, we have a huge number of event logs. To make your analysis easier, you can sort them. For example, we used the **Created Date/Time** column to sort our event logs. You can see partial results in the following figure:



Event ID	Security User ID	Created Date/T...	Event Description Summary	Level	Keywords	Provider Name
23	LocalSystem	7/14/2009 4:56:45 AM	Remote Desktop Services: Session logoff succeeded.	Information	0x1000000000000000	Microsoft-Windows-TerminalServices-Lo
101	LocalSystem	7/14/2009 4:56:45 AM	Windows Defender state updated.	Information	0x4000000000000000	Microsoft-Windows-Windows Defender
1002	LocalService	7/14/2009 4:56:45 AM	The Windows Resource Exhaustion Detector stopped.	Information	0x4000000010000000	Microsoft-Windows-Resource-Exhaustio
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5320	LocalSystem	10/19/2010 3:15:20 AM	Checking for Group Policy client extensions that are...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
5321	LocalSystem	10/19/2010 3:15:20 AM	A previous instance of the Group Policy Client Servic...	Information	0x4000000000000000	Microsoft-Windows-GroupPolicy
4001	LocalService	10/19/2010 3:15:25 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:25 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4002	LocalService	10/19/2010 3:15:26 AM		Information	0x4001200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:26 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10001	LocalService	10/19/2010 3:15:40 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4001	LocalService	10/19/2010 3:15:45 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:45 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
4002	LocalService	10/19/2010 3:15:46 AM		Information	0x4001200000000000	Microsoft-Windows-NetworkProfile
10000	LocalService	10/19/2010 3:15:46 AM		Information	0x4000200000000000	Microsoft-Windows-NetworkProfile
1006	LocalService	10/19/2010 3:15:57 AM	Router Advertisement settings have been changed...	Information	0x8000000000000000	Microsoft-Windows-DHCPv6-Client
1017	LocalSystem	10/19/2010 3:16:03 AM	A device will not be used for a ReadyBoost cache be...	Information	0x8000000000004000	Microsoft-Windows-ReadyBoost
1015	LocalSystem	10/19/2010 3:16:13 AM	Summary of ReadyBoot Performance.	Information	0x8000000000002000	Microsoft-Windows-ReadyBoost
1016	LocalSystem	10/19/2010 3:16:14 AM	Boot plan calculation completed.	Information	0x8000000000002000	Microsoft-Windows-ReadyBoost
306	LocalSystem	10/19/2010 3:17:25 AM	The BITS service loaded the job list from disk.		0x4000000000000000	Microsoft-Windows-Bits-Client

Figure 7.12. Sorted Event Logs records

Of course, you can use other columns to sort your logs, for example **Event ID** or **Event Description Summary**—it depends on the specific requirements of your case.

How it works...

Magnet AXIOM automatically finds available Windows Event Logs on a forensic image during the processing stage. As a result, the examiner has a list of all the logs with the ability to sort them according to different criteria.

See also

Magnet AXIOM for computers: https://www.magnetforensics.com/magnet-axiom/computers/

Event log recovery with EVTXtract

You already know how to export, sort and search through Windows event logs. Now it's time to learn how to recover deleted or corrupted event log artifacts. Thankfully, there is an open source tool by Willi Ballenthin that is capable of solving this problem: EVTXtract. The tool can recover EVTX fragments not only from RAW images, but also from unallocated space and memory dumps.

Getting ready

First of all, since EVTXtract is written in Python, make sure you have this installed on your workstation. If not, go to the official Python website, download and install it. Also, you will need **python-evtx,** which you can find in Willi's GitHub. Python-evtx is an EVTX parser, which is a dependence for EVTXtract. To install it, download and unpack the archive from GitHub, open Windows Command Prompt, choose the directory to which you unpacked the archive, and run the following command:

```
setup.py install
```

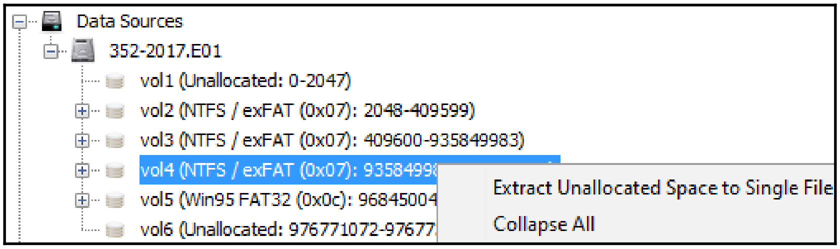
That's it; now you have python-evtx installed, and you are ready to install EVTXtract. The process is almost the same: download and unpack the archive from GitHub (but now use the EVTXtract download page), open the Windows Command Prompt, choose the directory to which you unpacked the archive, and run the following command:

```
setup.py install
```

We are done. Now you have `evtxtract.exe` in your Python 2 scripts folder - in our case it's *`C:\Python27\Scripts`* - and you are ready to use it.

How to do it...

First of all, you must decide what you are going to use as the source. You have three options: a disk image in RAW format, a memory dump, or an unallocated space. You have already created RAW disk images and memory images (dumps) in previous recipes, but what about unallocated space? You have already used **Autopsy**, and even recovered some data from an NTFS partition. But you can also use this tool to extract unallocated space to a separate file. To do this, go to **Data Sources**, right-click the partition you want to extract unallocated space from, and choose **Extract Unallocated Space to Single File.**



Data Sources
352-2017.E01
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-409599)
vol3 (NTFS / exFAT (0x07): 409600-935849983)
vol4 (NTFS / exFAT (0x07): 9358499
vol5 (Win95 FAT32 (0x0c): 96845004
vol6 (Unallocated: 976771072-97677

Figure 7.13. Extracting unallocated space to single file with Autopsy

Once unallocated space is extracted, you can use this file as the source for EVTXtract. To start the recovery process, use the following command:

```
evtxtract.exe image.raw > output.xml
```

Don't forget to change `image.raw` to the file of your choice. Once the process is finished, you can analyze and search through the output file.

How it works...

EVTXtract walks through a disk image (only RAW format is supported), a memory dump, or a file with extracted unallocated space (depending on the examiner's choice) and recovers EVTX fragments, saving them to an XML file.

See also

Python download page:
`https://www.python.org/downloads/`

Python-evtx download page:
`https://github.com/williballenthin/python-evtx`

EVTXtract download page:
`https://github.com/williballenthin/EVTXtract`

LNK file analysis with EnCase forensic

In our previous recipes, you have already learnt how to create a new case, add evidence files, and examine Windows recycle bin contents with EnCase Forensic. Now it's time to go even further, and meet the EnCase Evidence Processor, and especially the Windows Artifact Parser. This module enables a digital forensic examiner to parse different Windows forensic artifacts, including LNK files, automatically.

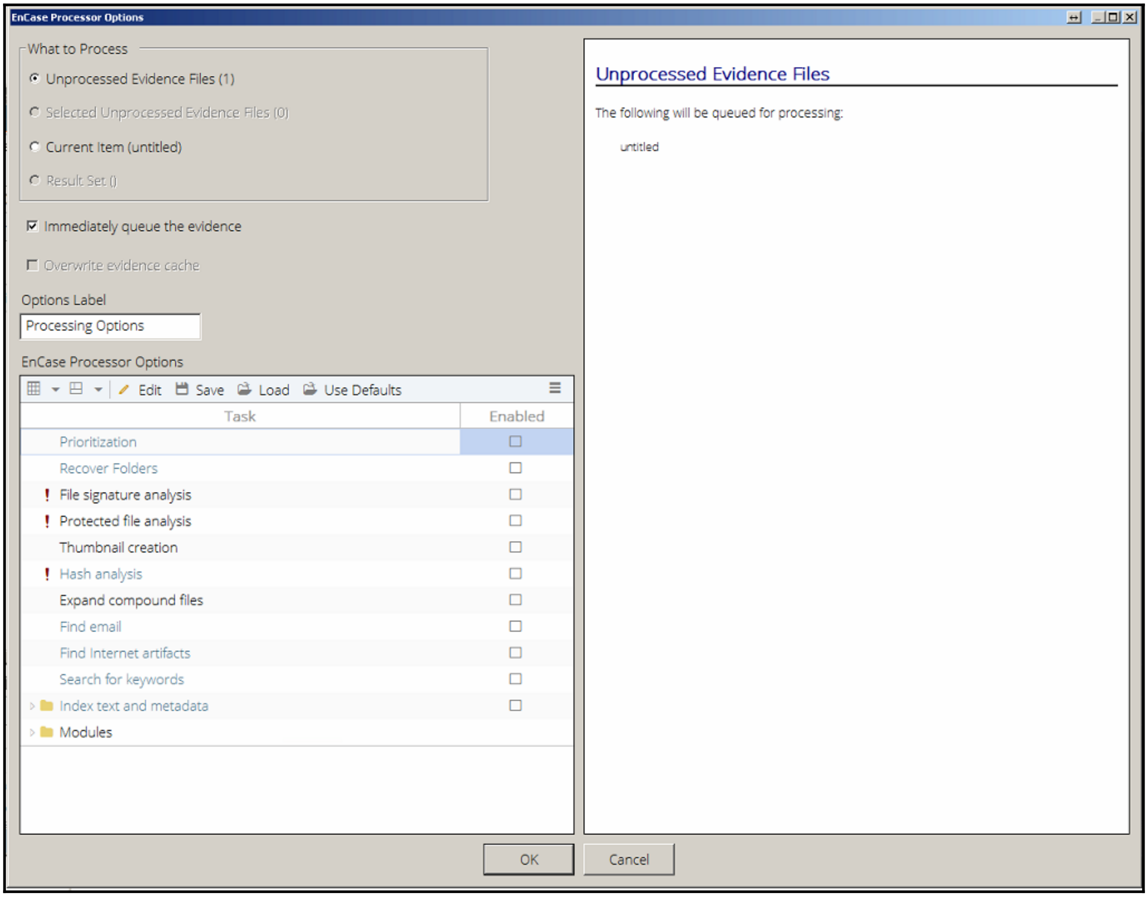
Getting ready

To use the EnCase Evidence Processor, you should create a case and add an evidence item. You already created a case to examine the recycle bin, so you can use that case here. If it's not available, create a new one and add an image to it. Once done, you are ready to use the EnCase Evidence Processor and the Windows Artifact Parser.

How to do it...

The steps for LNK files analysis are given as follows:

1. Once you have created a new case and added an evidence item, go to **Process Evidence - Process...** You will see the **EnCase Processor Options** window, as you can see in the following figure:



EnCase Processor Options

What to Process

● Unprocessed Evidence Files (1)

○ Selected Unprocessed Evidence Files (0)

○ Current Item (untitled)

○ Result Set ()

☑ Immediately queue the evidence

□ Overwrite evidence cache

Options Label: Processing Options

EnCase Processor Options

Task	Enabled
Prioritization	□
Recover Folders	□
! File signature analysis	□
! Protected file analysis	□
Thumbnail creation	□
! Hash analysis	□
Expand compound files	□
Find email	□
Find Internet artifacts	□
Search for keywords	□
Index text and metadata	□
Modules	

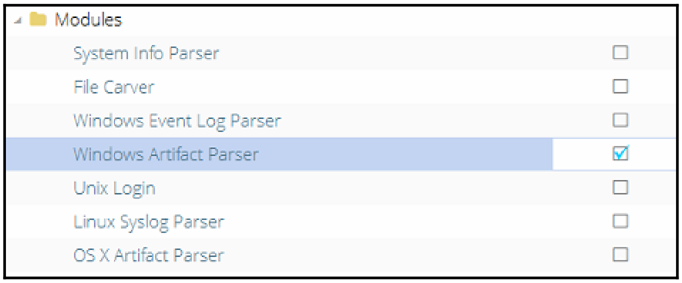
Unprocessed Evidence Files

The following will be queued for processing:

untitled

Figure 7.14. EnCase Processor Options

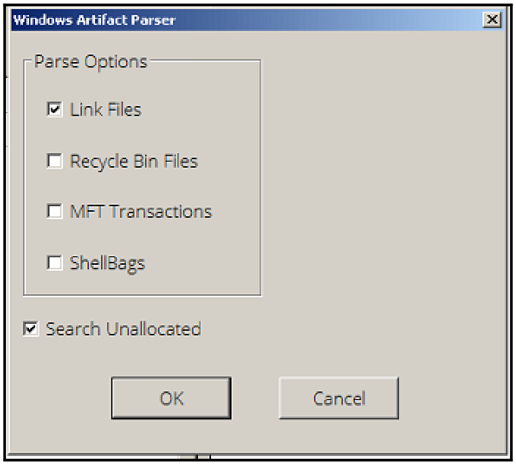
2. As you can see, we have quite a lot of options here: you can **Recover Folders**, **Find email**, **Find Internet artifacts**, and so on. But, for now, let's go to the **Modules** folder. You can see its contents in the following figure:



Modules
- System Info Parser □
- File Carver □
- Windows Event Log Parser □
- Windows Artifact Parser ☑
- Unix Login □
- Linux Syslog Parser □
- OS X Artifact Parser □

Figure 7.15. Modules folder contents

3. As it is already been said, this time we are interested in the **Windows Artifact Parser**. If you click on its name, you see the following options:



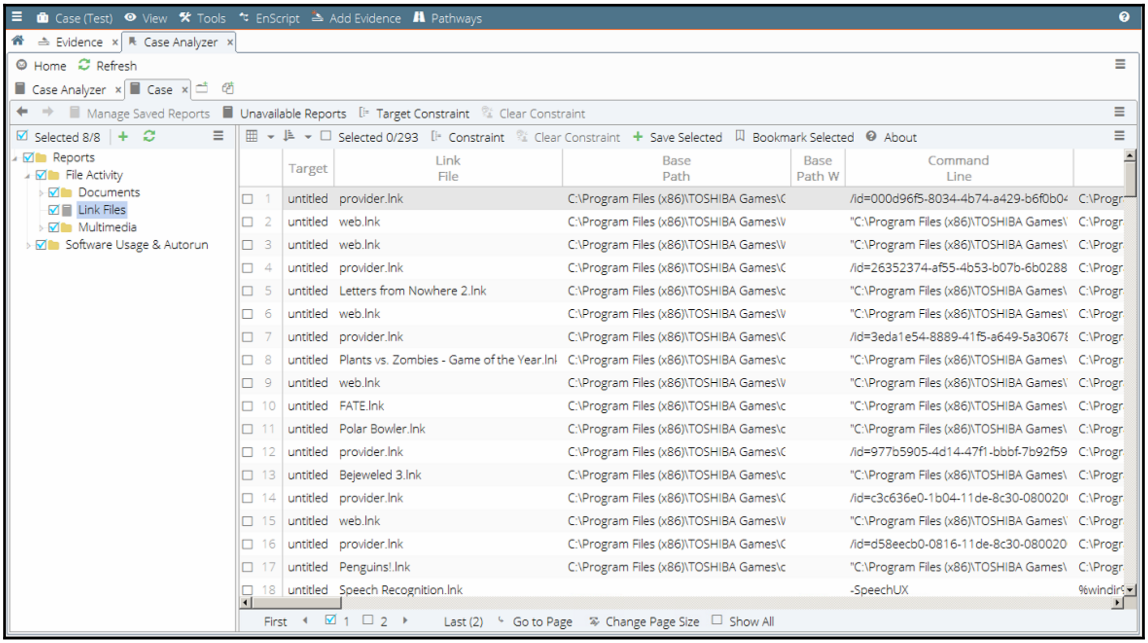
Windows Artifact Parser

Parse Options
- ☑ Link Files
- □ Recycle Bin Files
- □ MFT Transactions
- □ ShellBags

☑ Search Unallocated

Figure 7.16. Windows Artifact Parser options

4. This module is able to provide an examiner with information about **Link Files**, **Recycle Bin Files** (if you want them in the report, make sure you use this option), **MFT Transactions,** and **ShellBags**, including those extracted from an image's unallocated space (if you tick the **Search Unallocated** option).
5. This time, we are interested in parsing LNK files, so let's choose the **Link Files** option (don't forget to tick Search Unallocated, we don't want to miss anything!).
6. Once the processing is finished, go to **EnScript - Case Analyzer**. Here, you can find all the available LNK files with lots of metadata extracted by the Windows Artifact Parser. Take a look at the following figure for more details:



		Target	Link File	Base Path	Base Path W	Command Line	
☐	1	untitled	provider.lnk	C:\Program Files (x86)\TOSHIBA Games\C		/id=000d96f5-8034-4b74-a429-b6f0b04	C:\Progr
☐	2	untitled	web.lnk	C:\Program Files (x86)\TOSHIBA Games\W		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	3	untitled	web.lnk	C:\Program Files (x86)\TOSHIBA Games\W		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	4	untitled	provider.lnk	C:\Program Files (x86)\TOSHIBA Games\C		/id=26352374-af55-4b53-b07b-6b0288	C:\Progr
☐	5	untitled	Letters from Nowhere 2.lnk	C:\Program Files (x86)\TOSHIBA Games\c		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	6	untitled	web.lnk	C:\Program Files (x86)\TOSHIBA Games\W		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	7	untitled	provider.lnk	C:\Program Files (x86)\TOSHIBA Games\C		/id=3eda1e54-8889-41f5-a649-5a3067	C:\Progr
☐	8	untitled	Plants vs. Zombies - Game of the Year.lnl	C:\Program Files (x86)\TOSHIBA Games\c		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	9	untitled	web.lnk	C:\Program Files (x86)\TOSHIBA Games\W		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	10	untitled	FATE.lnk	C:\Program Files (x86)\TOSHIBA Games\c		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	11	untitled	Polar Bowler.lnk	C:\Program Files (x86)\TOSHIBA Games\c		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	12	untitled	provider.lnk	C:\Program Files (x86)\TOSHIBA Games\C		/id=977b5905-4d14-47f1-bbbf-7b92f59	C:\Progr
☐	13	untitled	Bejeweled 3.lnk	C:\Program Files (x86)\TOSHIBA Games\c		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	14	untitled	provider.lnk	C:\Program Files (x86)\TOSHIBA Games\C		/id=c3c636e0-1b04-11de-8c30-080020	C:\Progr
☐	15	untitled	web.lnk	C:\Program Files (x86)\TOSHIBA Games\W		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	16	untitled	provider.lnk	C:\Program Files (x86)\TOSHIBA Games\C		/id=d58eecb0-0816-11de-8c30-080020	C:\Progr
☐	17	untitled	Penguins!.lnk	C:\Program Files (x86)\TOSHIBA Games\c		"C:\Program Files (x86)\TOSHIBA Games\	C:\Progr
☐	18	untitled	Speech Recognition.lnk			-SpeechUX	%windir

Figure 7.17. Parsed LNK files

How it works...

Windows Artifact Parser walks through the image added to the case and extracts information from the LNK files it finds, including those from unallocated space if this option has been chosen by the examiner. Once the process is finished, the examiner can then analyze, bookmark, and add this information to their report.

See also

Windows Shortcut File format specification:
`https://github.com/libyal/liblnk/blob/master/documentation/Windows%20Shortcut%20File%20(LNK)%20format.asciidoc`

LNK file analysis with LECmd

LECmd is another great free and open source Windows forensic tool by Eric Zimmerman. It processes files really fast, and can be used for parsing both single LNK files and the folders that contain them. Also, it has quite a wide range of export options, including CSV and XML.

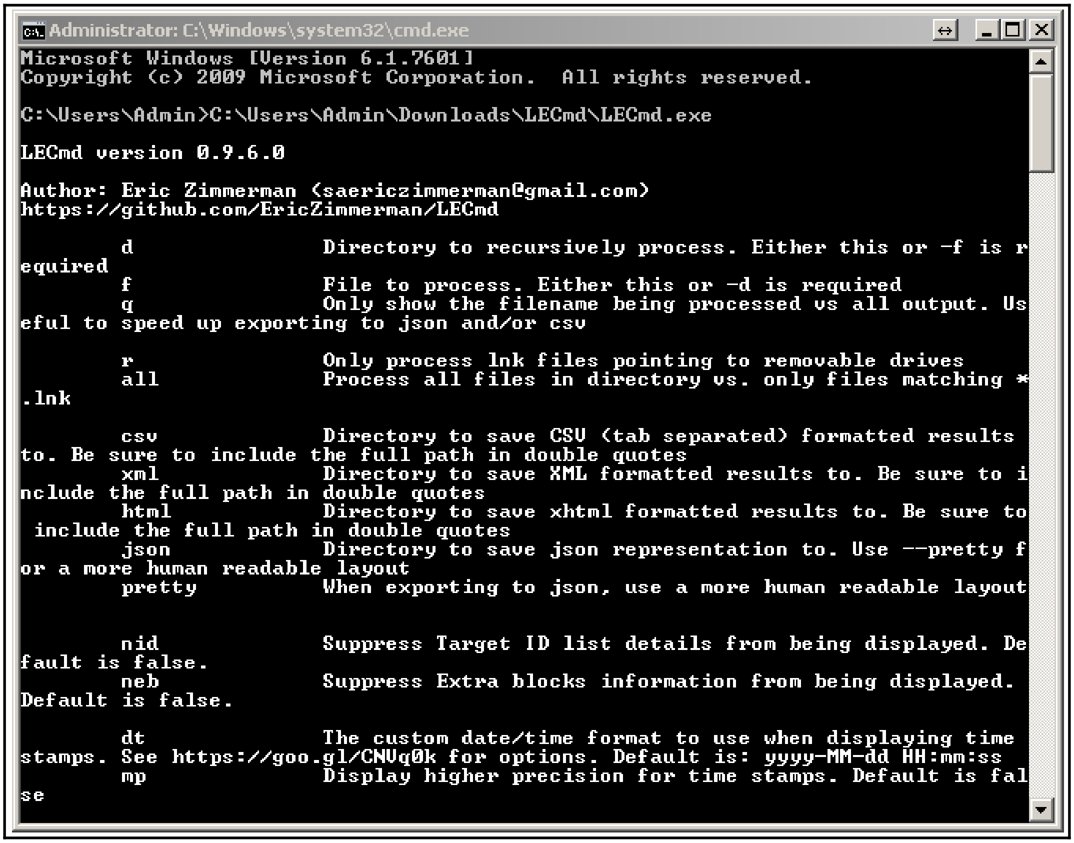
Getting ready

Go to the LECmd download page to get the archive with the tool. Unpack the archive you have downloaded, run the Windows Command Prompt, change the directory to the one you have just unpacked, and you are ready to go.

How to do it...

The steps for LNK files analysis with LECmd:

1. As we have already said, LECmd can process both single files and folders. If you want to extract information from a single file, use **-f** switch; if your target is a directory, use **-d** switch. If you are interested only in LNK files pointing to removable drives, you can use **-r** switch. The other available options can be seen in the following figure:



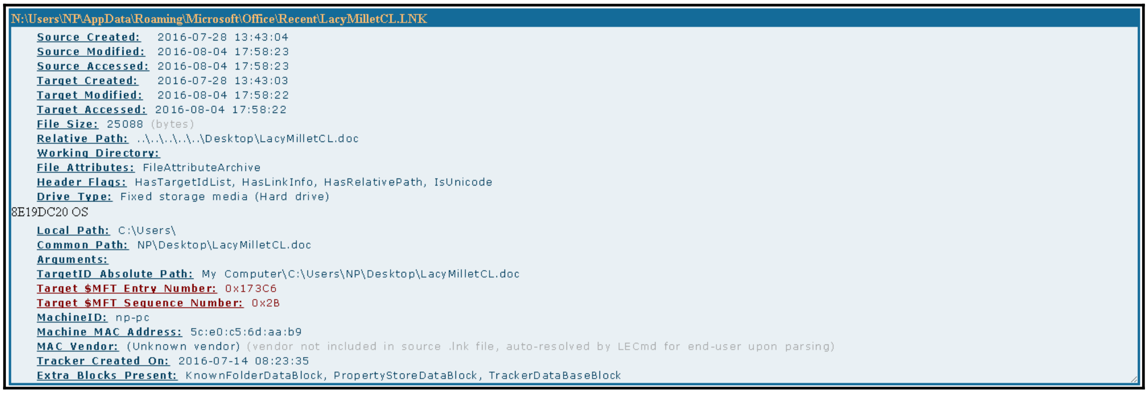
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Admin>C:\Users\Admin\Downloads\LECmd\LECmd.exe

LECmd version 0.9.6.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

        d               Directory to recursively process. Either this or -f is r
equired
        f               File to process. Either this or -d is required
        q               Only show the filename being processed vs all output. Us
eful to speed up exporting to json and/or csv

        r               Only process lnk files pointing to removable drives
        all             Process all files in directory vs. only files matching *
.lnk

        csv             Directory to save CSV (tab separated) formatted results
to. Be sure to include the full path in double quotes
        xml             Directory to save XML formatted results to. Be sure to i
nclude the full path in double quotes
        html            Directory to save xhtml formatted results to. Be sure to
 include the full path in double quotes
        json            Directory to save json representation to. Use --pretty f
or a more human readable layout
        pretty          When exporting to json, use a more human readable layout


        nid             Suppress Target ID list details from being displayed. De
fault is false.
        neb             Suppress Extra blocks information from being displayed.
Default is false.

        dt              The custom date/time format to use when displaying time
stamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss
        mp              Display higher precision for time stamps. Default is fal
se
```

Figure 7.18. LECmd options

2. If you want to run LECmd against a file or folder on a forensic image, first you should mount it. Thankfully, you already know how to do this. In our case, the main partition is mounted under `N:\`. Let's use LECmd against the `Roaming` folder and save the output formatted in xhtml. To do this, use the following command:

```
LECmd.exe -d "N:\Users\NP\AppData\Roaming" -xhtml
"C:\Users\Admin\Desktop\test.html
```

3. You can see part of the xhtml formatted output in the following figure:



```
N:\Users\NP\AppData\Roaming\Microsoft\Office\Recent\LacyMilletCL.LNK
    Source Created:   2016-07-28 13:43:04
    Source Modified:  2016-08-04 17:58:23
    Source Accessed:  2016-08-04 17:58:23
    Target Created:   2016-07-28 13:43:03
    Target Modified:  2016-08-04 17:58:22
    Target Accessed: 2016-08-04 17:58:22
    File Size: 25088 (bytes)
    Relative Path: ..\..\..\..\..\Desktop\LacyMilletCL.doc
    Working Directory:
    File Attributes: FileAttributeArchive
    Header Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, IsUnicode
    Drive Type: Fixed storage media (Hard drive)
8E19DC20 OS
    Local Path: C:\Users\
    Common Path: NP\Desktop\LacyMilletCL.doc
    Arguments:
    TargetID Absolute Path: My Computer\C:\Users\NP\Desktop\LacyMilletCL.doc
    Target $MFT Entry Number: 0x173C6
    Target $MFT Sequence Number: 0x2B
    MachineID: np-pc
    Machine MAC Address: 5c:e0:c5:6d:aa:b9
    MAC Vendor: (Unknown vendor) (vendor not included in source .lnk file, auto-resolved by LECmd for end-user upon parsing)
    Tracker Created On: 2016-07-14 08:23:35
    Extra Blocks Present: KnownFolderDataBlock, PropertyStoreDataBlock, TrackerDataBaseBlock
```

Figure 7.19. A part of LECmd xhtml formatted output

4. As you can see in the preceding figure, LECmd extracts lots of information from LNK files. For example, we have MAC (modified, accessed, created) times both for the LNK file and the target file (in our case, LacyMilletCL.doc), as well as the target file's size, absolute path, and even computer ID and MAC address.

How it works...

LECmd walks through a folder or a single file, extracts information from available LNK files, and saves the output to the format chosen by the examiner.

See also

LECmd download page:
`https://ericzimmerman.github.io/`

Introducing LECmd:
`https://binaryforay.blogspot.ru/2016/02/introducing-lecmd.html`

Shell Link (.LNK) Binary File Format:
`https://msdn.microsoft.com/en-us/library/dd871305.aspx`

LNK file analysis with Link Parser

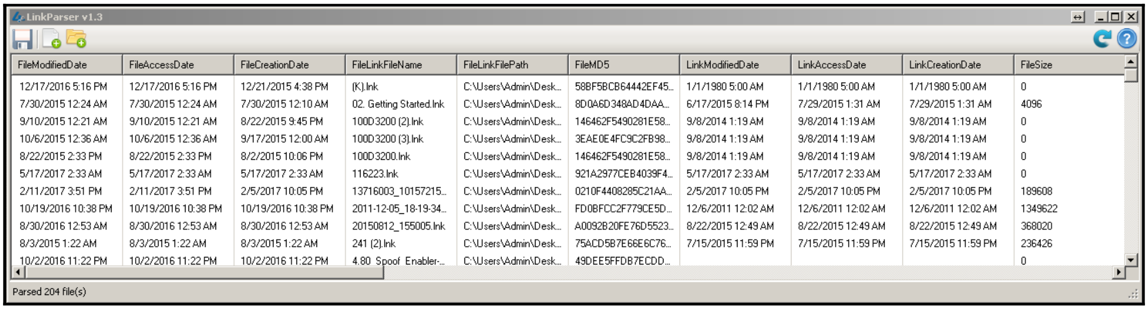
Link Parser is another free tool that can be used by digital forensic examiners for Microsoft Shell Link files. It is developed by 4Discovery, and is capable of parsing a single LNK file, multiple selected files, or recursively over a folder or mounted forensic image.

Getting ready

Go to the Link Parser page on 4Discovery's website (you can find the link in the See Also section), and download an archive with the tool - at the time of writing the most recent version is 1.3. Unpack the archive, and you are ready to go.

How to do it...

Start `LinkParser.exe`, click on the folder icon, and choose a folder with the LNK files you want the tool to parse. In our case, it's `C:\Users\{username}\AppData\Roaming\Microsoft\Windows\Recent` - this folder contains recently used items; we exported it from a forensic image using FTK Imager. Link Parser has extracted data from 204 LNK files, as seen in the following figure:



FileModifiedDate	FileAccessDate	FileCreationDate	FileLinkFileName	FileLinkFilePath	FileMD5	LinkModifiedDate	LinkAccessDate	LinkCreationDate	FileSize
12/17/2016 5:16 PM	12/17/2016 5:16 PM	12/21/2015 4:38 PM	(K).lnk	C:\Users\Admin\Desk...	58BF5BCB64442EF45...	1/1/1980 5:00 AM	1/1/1980 5:00 AM	1/1/1980 5:00 AM	0
7/30/2015 12:24 AM	7/30/2015 12:24 AM	7/30/2015 12:10 AM	02. Getting Started.lnk	C:\Users\Admin\Desk...	8D0A6D348AD4DAA...	6/17/2015 8:14 PM	7/29/2015 1:31 AM	7/29/2015 1:31 AM	4096
9/10/2015 12:21 AM	9/10/2015 12:21 AM	8/22/2015 9:45 PM	100D3200 (2).lnk	C:\Users\Admin\Desk...	146462F5490281E58...	9/8/2014 1:19 AM	9/8/2014 1:19 AM	9/8/2014 1:19 AM	0
10/6/2015 12:36 AM	10/6/2015 12:36 AM	9/17/2015 12:00 AM	100D3200 (3).lnk	C:\Users\Admin\Desk...	3EAE0E4FC9C2FB98...	9/8/2014 1:19 AM	9/8/2014 1:19 AM	9/8/2014 1:19 AM	0
8/22/2015 2:33 PM	8/22/2015 2:33 PM	8/2/2015 10:06 PM	100D3200.lnk	C:\Users\Admin\Desk...	146462F5490281E58...	9/8/2014 1:19 AM	9/8/2014 1:19 AM	9/8/2014 1:19 AM	0
5/17/2017 2:33 AM	5/17/2017 2:33 AM	5/17/2017 2:33 AM	116223.lnk	C:\Users\Admin\Desk...	921A2977CEB4039F4...	5/17/2017 2:33 AM	5/17/2017 2:33 AM	5/17/2017 2:33 AM	0
2/11/2017 3:51 PM	2/11/2017 3:51 PM	2/5/2017 10:05 PM	13716003_10157215...	C:\Users\Admin\Desk...	0210F4408285C21AA...	2/5/2017 10:05 PM	2/5/2017 10:05 PM	2/5/2017 10:05 PM	189608
10/19/2016 10:38 PM	10/19/2016 10:38 PM	10/19/2016 10:38 PM	2011-12-05_18-19-34...	C:\Users\Admin\Desk...	FD0BFCC2F779CE5D...	12/6/2011 12:02 AM	12/6/2011 12:02 AM	12/6/2011 12:02 AM	1349622
8/30/2016 12:53 AM	8/30/2016 12:53 AM	8/30/2016 12:53 AM	20150812_155005.lnk	C:\Users\Admin\Desk...	A0092B20FE76D5523...	8/22/2015 12:49 AM	8/22/2015 12:49 AM	8/22/2015 12:49 AM	368020
8/3/2015 1:22 AM	8/3/2015 1:22 AM	8/3/2015 1:22 AM	241 (2).lnk	C:\Users\Admin\Desk...	75ACD5B7E66E6C76...	7/15/2015 11:59 PM	7/15/2015 11:59 PM	7/15/2015 11:59 PM	236426
10/2/2016 11:22 PM	10/2/2016 11:22 PM	10/2/2016 11:22 PM	4.80 Spoof Enabler-...	C:\Users\Admin\Desk...	49DEE5FFDB7ECDD...				0

Parsed 204 file(s)

Figure 7.20. Link Parser output

Link Parser extracts a huge amount of data from LNK files - more than 30 attributes, including **Volume Serial Number**, **Volume Label**, **Volume ID**, and more.

All parsed attributes can be easily exported to `CSV`. To do this, click the floppy disk icon, choose **Export file name,** and select a location. After this, you can easily import exported data into your favorite spreadsheet application.

How it works...

Link Parser walks through a folder or single LNK file chosen by the examiner and extracts more than 30 attributes from available LNK files. Parsed data can be exported to a CSV file.

See also

Link Parser download page:

`http://www.4discovery.com/our-tools/`

Prefetch file analysis with Magnet AXIOM

If you have been following the recipes in this book, you already know what Magnet AXIOM is, and have even used it for forensic analysis of some Windows artifacts. AXIOM is a really good tool, so we are going to continue to show you how to use it for parsing and analysis of different useful operating system artifacts: this time, prefetch files.

Getting ready

As you have already used AXIOM, there is no need to install it - it's already on your workstation. If, for some reason, it's not, refer to the **See Also** section to learn how to get a trial version of the tool. Also, you will need an evidence source: a forensic image or a folder with prefetch files (this is located in `C:\Windows\Prefetch`). As soon as you have located one of the options, you are ready to go.

How to do it...

The steps for Prefetch file analysis with Magnet AXIOM:

1. Create a new case and go to **Load evidence**. You have five options here: **CONNECTED DRIVE**, **FILES & FOLDERS**, **COMPUTER IMAGE**, **VOLUME SHADOW COPY,** and **MOBILE DEVICES**, as you can see in the following figure:

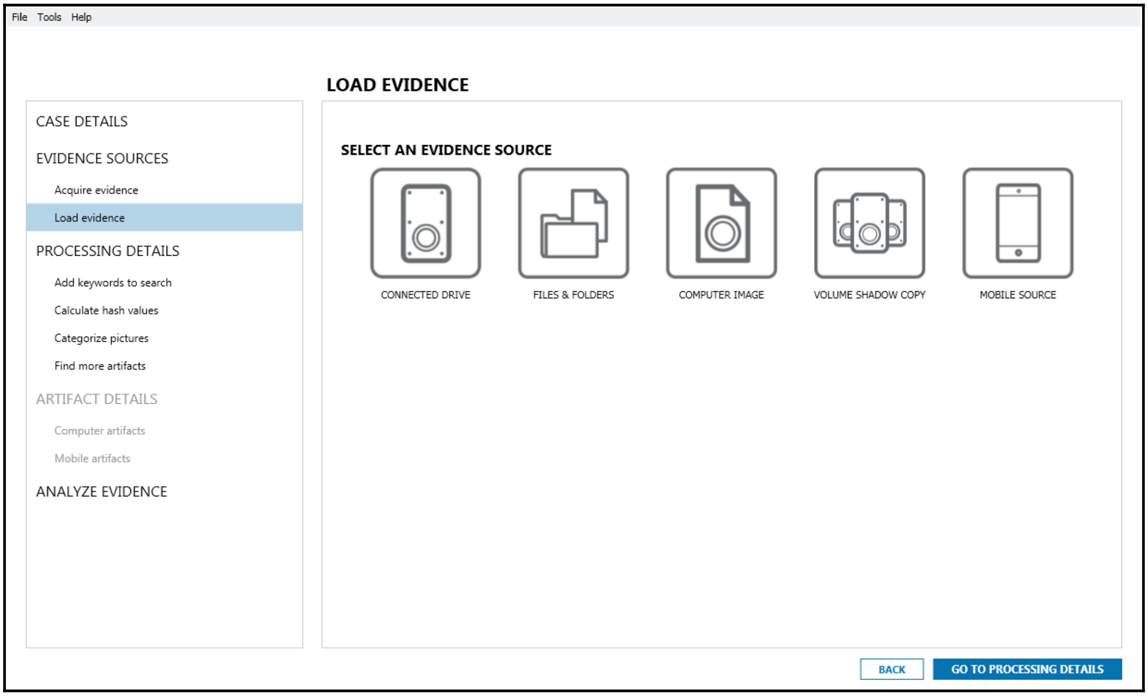
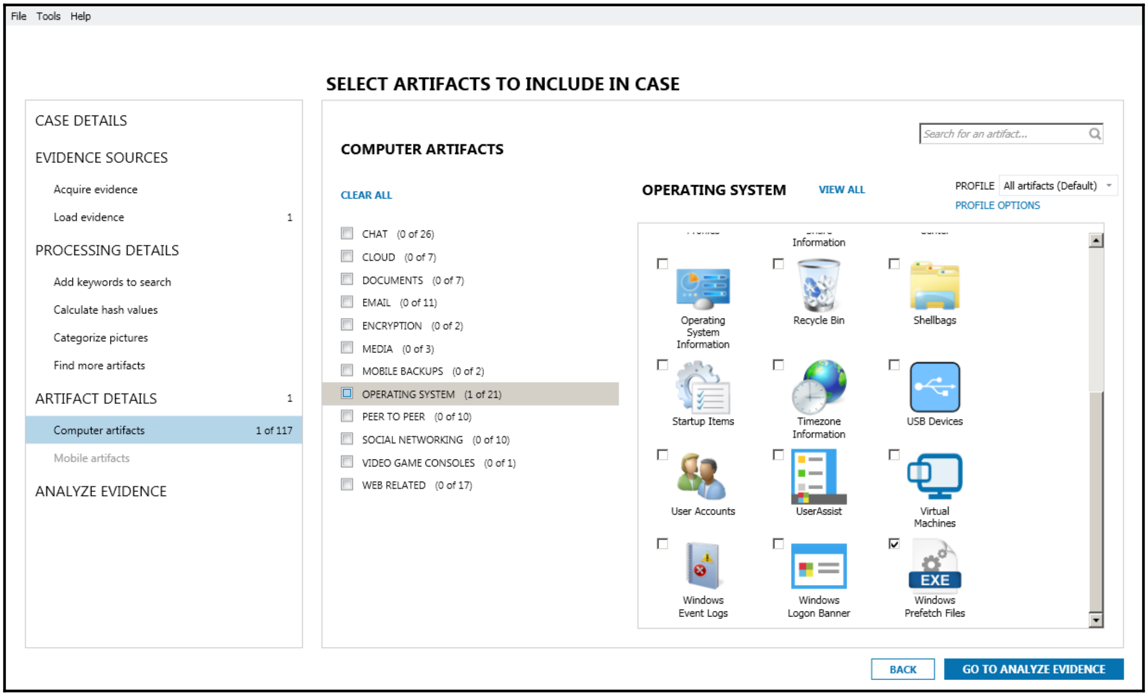


Figure 7.21. Load evidence options

2. As mentioned before, you can use a forensic image or a previously exported folder with prefetch files. If you prefer the first option, choose **COMPUTER IMAGE;** if the second, choose **FILES & FOLDERS**. In our case, it's a folder, which has been chosen with the help of the AXIOM folder browser.

3. Now, let's go to the artifact details. As we are interested in prefetches, let's choose only these artifacts from the list. Click the **CUSTOMIZE COMPUTER ARTIFACTS** button, then **CLEAR ALL**, go to **OPERATING SYSTEM,** and tick the **Windows Prefetch Files** option. You can see how this works in the figure below:



SELECT ARTIFACTS TO INCLUDE IN CASE

CASE DETAILS

EVIDENCE SOURCES

Acquire evidence

Load evidence 1

PROCESSING DETAILS

Add keywords to search

Calculate hash values

Categorize pictures

Find more artifacts

ARTIFACT DETAILS 1

Computer artifacts 1 of 117

Mobile artifacts

ANALYZE EVIDENCE

COMPUTER ARTIFACTS

Search for an artifact...

CLEAR ALL

□ CHAT (0 of 26)
□ CLOUD (0 of 7)
□ DOCUMENTS (0 of 7)
□ EMAIL (0 of 11)
□ ENCRYPTION (0 of 2)
□ MEDIA (0 of 3)
□ MOBILE BACKUPS (0 of 2)
□ OPERATING SYSTEM (1 of 21)
□ PEER TO PEER (0 of 10)
□ SOCIAL NETWORKING (0 of 10)
□ VIDEO GAME CONSOLES (0 of 1)
□ WEB RELATED (0 of 17)

OPERATING SYSTEM VIEW ALL

PROFILE All artifacts (Default)

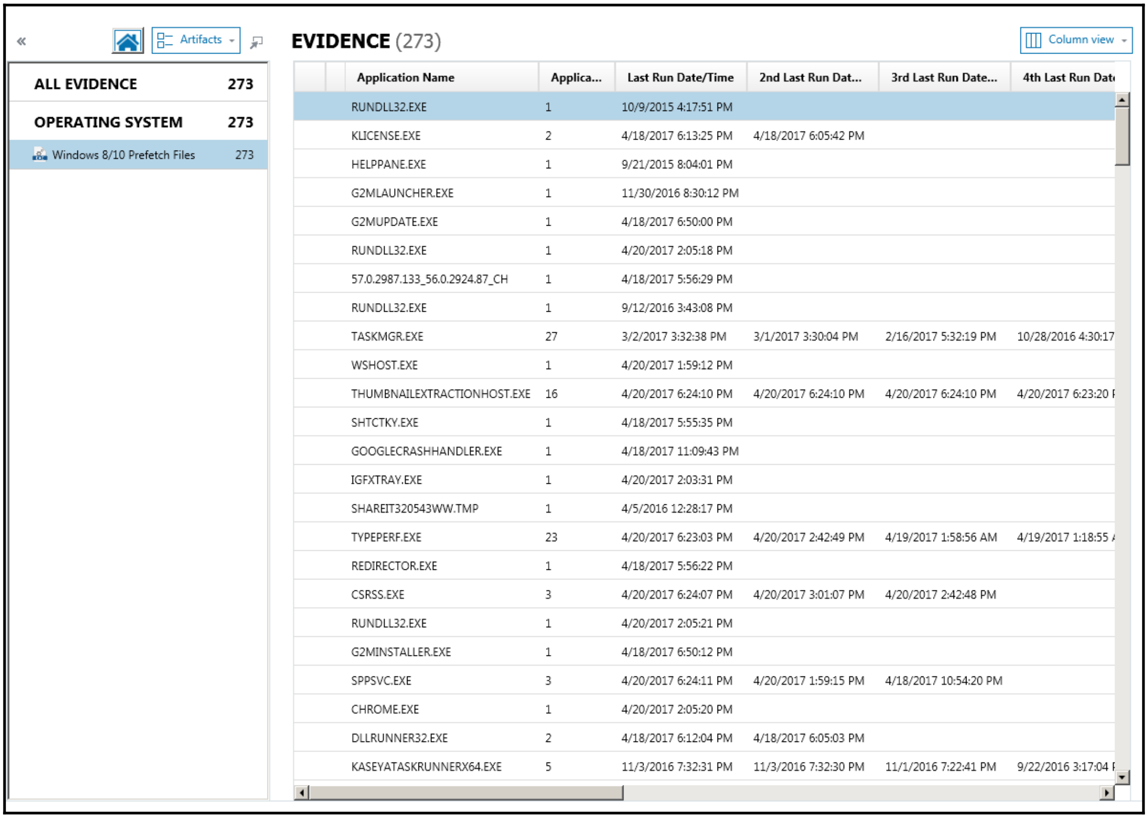
PROFILE OPTIONS

Information

□ Operating System Information
□ Recycle Bin
□ Shellbags
□ Startup Items
□ Timezone Information
□ USB Devices
□ User Accounts
□ UserAssist
□ Virtual Machines
□ Windows Event Logs
□ Windows Logon Banner
☑ Windows Prefetch Files

Figure 7.22. Selecting artifacts to include in case

4. So, now, we are ready to start analyzing the evidence. We have chosen only a folder with prefetch files, so very soon we can view parsing results in AXIOM Examine. Once the processing phase is finished, you are ready to view and analyze the results, as shown in the following figure:



ALL EVIDENCE 273

OPERATING SYSTEM 273

Windows 8/10 Prefetch Files 273

EVIDENCE (273)

Application Name	Applica...	Last Run Date/Time	2nd Last Run Dat...	3rd Last Run Date...	4th Last Run Date
RUNDLL32.EXE	1	10/9/2015 4:17:51 PM			
KLICENSE.EXE	2	4/18/2017 6:13:25 PM	4/18/2017 6:05:42 PM		
HELPPANE.EXE	1	9/21/2015 8:04:01 PM			
G2MLAUNCHER.EXE	1	11/30/2016 8:30:12 PM			
G2MUPDATE.EXE	1	4/18/2017 6:50:00 PM			
RUNDLL32.EXE	1	4/20/2017 2:05:18 PM			
57.0.2987.133_56.0.2924.87_CH	1	4/18/2017 5:56:29 PM			
RUNDLL32.EXE	1	9/12/2016 3:43:08 PM			
TASKMGR.EXE	27	3/2/2017 3:32:38 PM	3/1/2017 3:30:04 PM	2/16/2017 5:32:19 PM	10/28/2016 4:30:17
WSHOST.EXE	1	4/20/2017 1:59:12 PM			
THUMBNAILEXTRACTIONHOST.EXE	16	4/20/2017 6:24:10 PM	4/20/2017 6:24:10 PM	4/20/2017 6:24:10 PM	4/20/2017 6:23:20
SHTCTKY.EXE	1	4/18/2017 5:55:35 PM			
GOOGLECRASHHANDLER.EXE	1	4/18/2017 11:09:43 PM			
IGFXTRAY.EXE	1	4/20/2017 2:03:31 PM			
SHAREIT320543WW.TMP	1	4/5/2016 12:28:17 PM			
TYPEPERF.EXE	23	4/20/2017 6:23:03 PM	4/20/2017 2:42:49 PM	4/19/2017 1:58:56 AM	4/19/2017 1:18:55
REDIRECTOR.EXE	1	4/18/2017 5:56:22 PM			
CSRSS.EXE	3	4/20/2017 6:24:07 PM	4/20/2017 3:01:07 PM	4/20/2017 2:42:48 PM	
RUNDLL32.EXE	1	4/20/2017 2:05:21 PM			
G2MINSTALLER.EXE	1	4/18/2017 6:50:12 PM			
SPPSVC.EXE	3	4/20/2017 6:24:11 PM	4/20/2017 1:59:15 PM	4/18/2017 10:54:20 PM	
CHROME.EXE	1	4/20/2017 2:05:20 PM			
DLLRUNNER32.EXE	2	4/18/2017 6:12:04 PM	4/18/2017 6:05:03 PM		
KASEYATASKRUNNERX64.EXE	5	11/3/2016 7:32:31 PM	11/3/2016 7:32:30 PM	11/1/2016 7:22:41 PM	9/22/2016 3:17:04

Figure 7.23. Prefetch files parsing results

As you can see, we can get the number of runs for each program, and also the timestamps of up to eight recent runs. A very valuable piece of information, especially for malware forensics!

How it works...

Magnet AXIOM searches for prefetch files and extracts information about the run count and the timestamps of up to eight recent runs.

See also

Try Magnet AXIOM Free for 30 Days:

`https://www.magnetforensics.com/try-magnet-axiom-free-30-days/`

Windows Prefetch File (PF) format:

`https://github.com/libyal/libscca/blob/master/documentation/Windows%20Prefetch%20File%20(PF)%20format.asciidoc`

Forensic Analysis of Prefetch files in Windows:

`https://www.magnetforensics.com/computer-forensics/forensic-analysis-of-prefetch-files-in-windows/`

Prefetch file parsing with PECmd

If you have found some suspicious prefetch files and want to perform in-depth analysis, there is another tool by Eric Zimmerman that can help you - PECmd. This is a free and fast command-line tool capable of parsing Windows Prefetch files, both in old and new formats. In this recipe, we will show you how to extract valuable data from prefetches with the help of this tool.

Getting ready

Go to the PECmd download page, get the archive with the tool - at the time of writing, the most recent version is 0.9.0.0 - and unpack it. Also, you will need a prefetch file to work with, or a folder with such a file. As you already know, it can be exported from a forensic image with a tool of your choice. As soon as you get it, open the Windows Command Prompt, and you are ready to go!

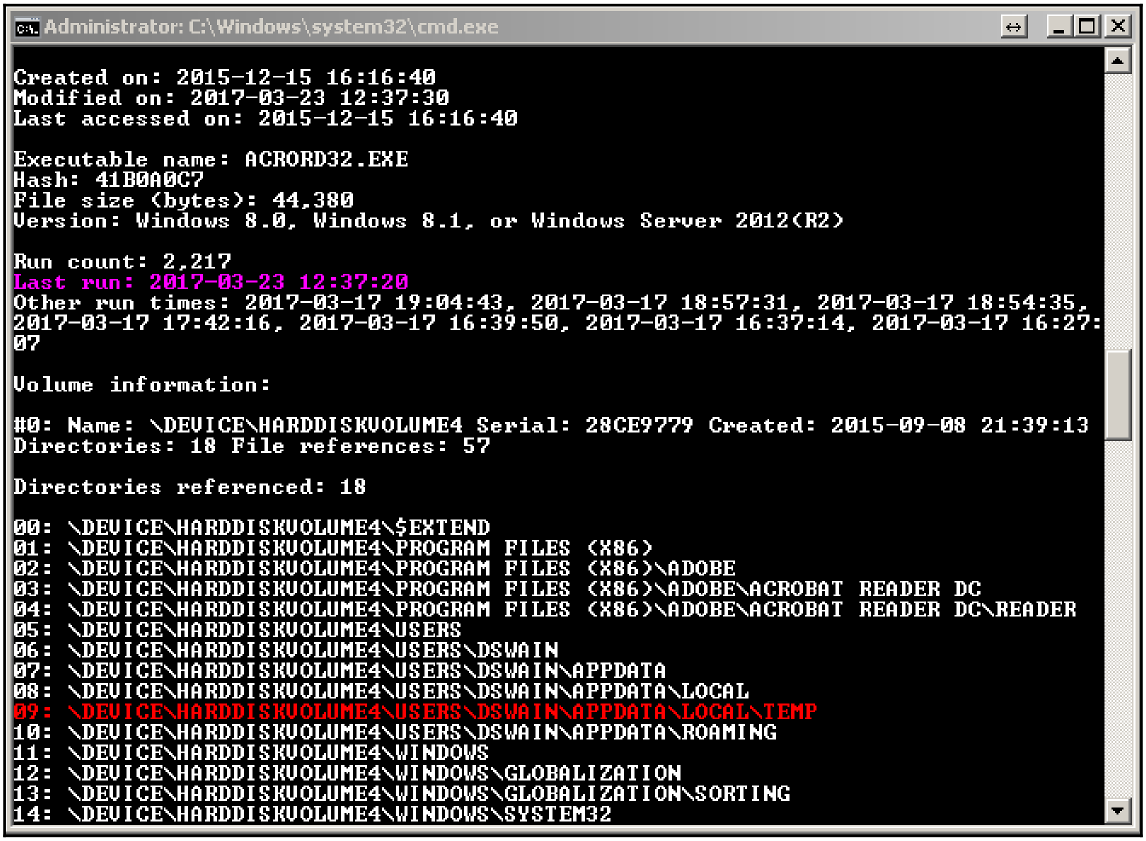
How to do it...

The steps for prefetch file parsing with PECmd are as follows:

1. Using the Windows Command Prompt, change the directory to the one where you unpacked the archive, and run the following command:

   ```
   PECmd.exe -f
   C:\Users\Admin\Desktop\Prefetch\ACRORD32.EXE-41B0A0C7.pf
   ```

   You will see the output very shortly, as in the following figure:



```
Created on: 2015-12-15 16:16:40
Modified on: 2017-03-23 12:37:30
Last accessed on: 2015-12-15 16:16:40

Executable name: ACRORD32.EXE
Hash: 41B0A0C7
File size (bytes): 44,380
Version: Windows 8.0, Windows 8.1, or Windows Server 2012(R2)

Run count: 2,217
Last run: 2017-03-23 12:37:20
Other run times: 2017-03-17 19:04:43, 2017-03-17 18:57:31, 2017-03-17 18:54:35,
2017-03-17 17:42:16, 2017-03-17 16:39:50, 2017-03-17 16:37:14, 2017-03-17 16:27:
07

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME4 Serial: 28CE9779 Created: 2015-09-08 21:39:13
Directories: 18 File references: 57

Directories referenced: 18

00: \DEVICE\HARDDISKVOLUME4\$EXTEND
01: \DEVICE\HARDDISKVOLUME4\PROGRAM FILES (X86)
02: \DEVICE\HARDDISKVOLUME4\PROGRAM FILES (X86)\ADOBE
03: \DEVICE\HARDDISKVOLUME4\PROGRAM FILES (X86)\ADOBE\ACROBAT READER DC
04: \DEVICE\HARDDISKVOLUME4\PROGRAM FILES (X86)\ADOBE\ACROBAT READER DC\READER
05: \DEVICE\HARDDISKVOLUME4\USERS
06: \DEVICE\HARDDISKVOLUME4\USERS\DSWAIN
07: \DEVICE\HARDDISKVOLUME4\USERS\DSWAIN\APPDATA
08: \DEVICE\HARDDISKVOLUME4\USERS\DSWAIN\APPDATA\LOCAL
09: \DEVICE\HARDDISKVOLUME4\USERS\DSWAIN\APPDATA\LOCAL\TEMP
10: \DEVICE\HARDDISKVOLUME4\USERS\DSWAIN\APPDATA\ROAMING
11: \DEVICE\HARDDISKVOLUME4\WINDOWS
12: \DEVICE\HARDDISKVOLUME4\WINDOWS\GLOBALIZATION
13: \DEVICE\HARDDISKVOLUME4\WINDOWS\GLOBALIZATION\SORTING
14: \DEVICE\HARDDISKVOLUME4\WINDOWS\SYSTEM32
```

Figure 7.24. PECmd output

2. As you can see in the preceding figure, we can get the executable name, its run count, timestamps of the last eight runs, and even lists of directories and files references. Not bad, right?

   You can also parse all files in a directory recursively. To do this, use the following command:

   ```
   PECmd.exe –d C:\Users\Admin\Desktop\Prefetch\
   ```

The tool is tiny, but really powerful, and is highly recommended for use in Windows Prefetch analysis in your forensic examinations.

How it works...

PECmd extracts available information from a prefetch file, or multiple prefetch files, in a folder specified by the user. The information includes the total number of runs, timestamps for recent runs, directories and files references, and more.

See also

PECmd download page:

`https://ericzimmerman.github.io/`

Introducing PECmd:

`https://binaryforay.blogspot.ru/2016/01/introducing-pecmd.html`

Prefetch file recovery with Windows Prefetch Carver

If you want to try to carve Windows Prefetch files from arbitrary binary data, there is a tool for you - Windows Prefetch Carver by Adam Witt. It can be used for prefetch carving from a drive's unallocated space or a memory image, for example. In this recipe we will show you how to use it.

Getting ready

Go to the Windows Prefetch Carver GitHub page (presented in the See Also section), and download the archive using the green Clone or Download button. Unpack the archive, start the Windows Command Prompt, and change the directory to the folder you unpacked it into. You are ready to go!

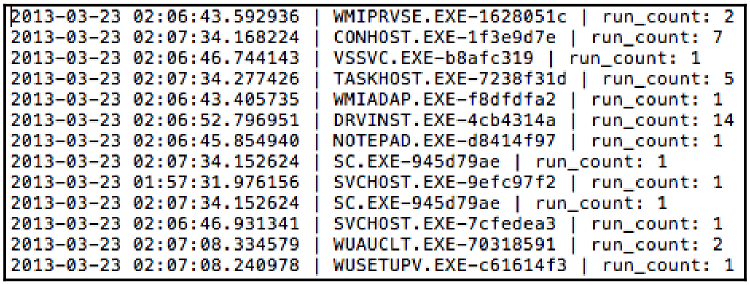
How to do it...

The steps for prefetch file recovery with Windows Prefetch Carver are as follows:

1. For this recipe, we used a memory image from a Windows 7 system. The image is called `joshua1.vmem` - you can find the download link for this memory image in the *See Also* section. Now let's use the tool. Type the following command:

   ```
   prefetch-carve.py -f joshua1.vmem -o output.txt
   ```

   As the result, you'll get an output file with carved data, as in the figure below:

   ```
   2013-03-23 02:06:43.592936 | WMIPRVSE.EXE-1628051c | run_count: 2
   2013-03-23 02:07:34.168224 | CONHOST.EXE-1f3e9d7e | run_count: 7
   2013-03-23 02:06:46.744143 | VSSVC.EXE-b8afc319 | run_count: 1
   2013-03-23 02:07:34.277426 | TASKHOST.EXE-7238f31d | run_count: 5
   2013-03-23 02:06:43.405735 | WMIADAP.EXE-f8dfdfa2 | run_count: 1
   2013-03-23 02:06:52.796951 | DRVINST.EXE-4cb4314a | run_count: 14
   2013-03-23 02:06:45.854940 | NOTEPAD.EXE-d8414f97 | run_count: 1
   2013-03-23 02:07:34.152624 | SC.EXE-945d79ae | run_count: 1
   2013-03-23 01:57:31.976156 | SVCHOST.EXE-9efc97f2 | run_count: 1
   2013-03-23 02:07:34.152624 | SC.EXE-945d79ae | run_count: 1
   2013-03-23 02:06:46.931341 | SVCHOST.EXE-7cfedea3 | run_count: 1
   2013-03-23 02:07:08.334579 | WUAUCLT.EXE-70318591 | run_count: 2
   2013-03-23 02:07:08.240978 | WUSETUPV.EXE-c61614f3 | run_count: 1
   ```

   Figure 7.25. Windows Prefetch Carver output

2. As you can see, the tool carved 13 records: timestamps, file names, and run counts are presented. There are a few output formats supported, including CSV and mactime. Run the script without arguments to learn how to save carved data in different formats.

How it works...

Windows Prefetch Carver scans a piece of arbitrary binary data of the examiner's choice, and extracts Windows Prefetch file artifacts, including timestamps, file names, and run counts.

See also

Windows Prefetch Carver GitHub page: `https://github.com/PoorBillionaire/Windows-Prefetch-Carver`

Windows 7 memory image download page: `http://jessekornblum.livejournal.com/293291.html`

8

Web Browser Forensics

In this chapter, we will cover the following recipes:

- Mozilla Firefox analysis with BlackBag BlackLight
- Google Chrome analysis with Magnet AXIOM
- Microsoft Internet Explorer and Microsoft Edge analysis with Belkasoft Evidence Center
- Extracting web browser data from Pagefile.sys

Introduction

It is hard to imagine a case where web browser artifacts are useless. Child abuse material, intellectual property theft, cyber harassment, malware - browser artifacts will help to solve all sorts of cases. Nowadays, a huge number of web browsers are available. Some provide their users with increased privacy options, others do not. But even if the suspect uses a private browser, such as notorious Tor, a computer forensic examiner is able to extract some data, for example from swap and hibernation files (check the last recipe in this chapter) or a memory dump.

In this chapter, we will show you how to perform web browser forensics with some forensic tools you have already dealt with, such as Magnet AXIOM and Belkasoft Evidence Center, and some new ones, such as BlackBag's BlackLight.

Finally, you will learn how to defeat some anti-forensic techniques using swap (`pagefile.sys` and `swapfile.sys`) and hibernation files. Let's go!

Mozilla Firefox analysis with BlackBag's BlackLight

BlackBag's BlackLight is a very powerful digital forensic tool which we usually use for Mac OS X (macOS) forensicating. But, of course, Mac is not the only platform it supports. You can also use it for Android, iOS, and Windows forensics. What's more, you can use BlackLight both on Windows and macOS workstations, meaning that you can analyze Windows forensic images on a Mac! In this recipe, we will show you how to use BlackLight for Mozilla Firefox forensics.

Getting ready

If you are not a licensed user of BlackLight, you can request a trial licence on the BlackBag website. Use the REQUEST TRIAL button on the BlackLight page, fill in your personal information, such as first and last names, phone number, city, email, and so on, and click on SUBMIT. You'll get your trial key and product download links via email, so make sure you have submitted your real email, ideally a government or business one.

Now you need to get a folder with Firefox files for analysis. If you have a Windows XP system, look here:

```
C:\Documents and Settings\%USERNAME%\Application Data\Mozilla\Firefox\
```

If you are dealing with a Windows Vista system (or later), look here:

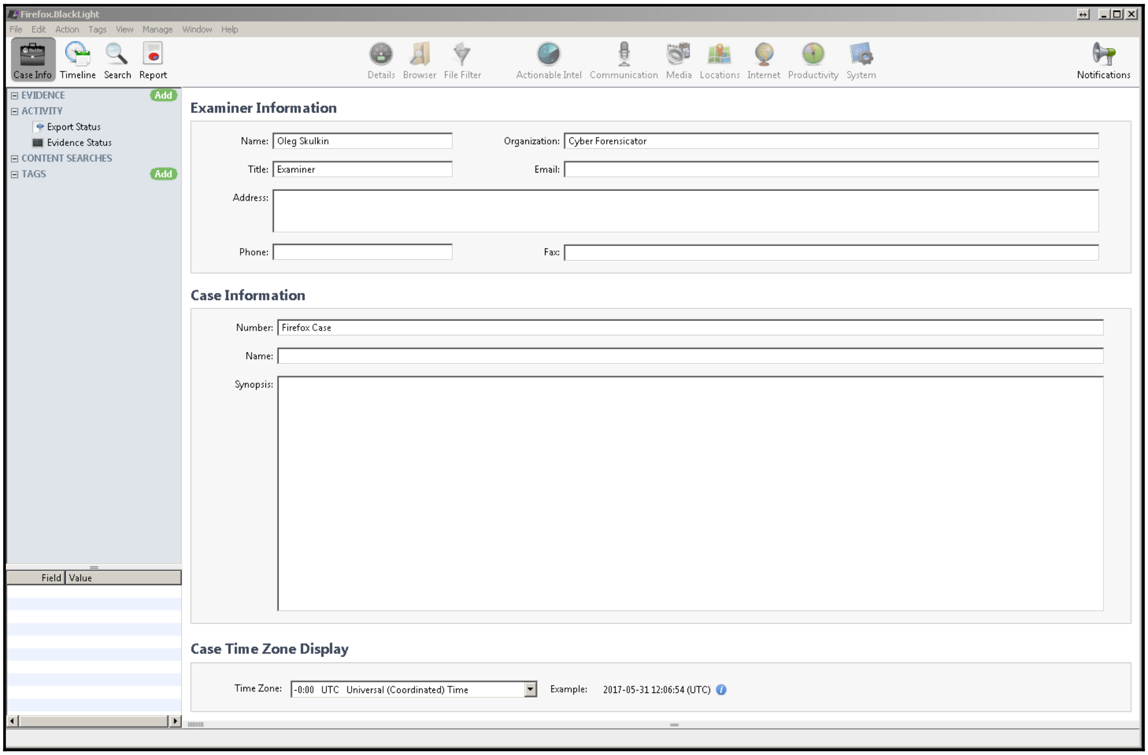
```
C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE%.defau
lt
```

Among other files, you'll find a bunch of valuable SQLite databases. These databases contain information about browsing history, downloads and so on, and BlackLight will help us to extract and analyze this data.

How to do it...

The steps for Mozilla Firefox analysis are as follows:

1. Open BlackLight and create a new case. To do this, go to **File - New Case**, or just click on the **New...** button, and choose your case location. Once you have saved the case, you can start filling in the necessary fields and choose the right time zone, as shown in the following figure:



Examiner Information

Name: Oleg Skulkin

Organization: Cyber Forensicator

Title: Examiner

Email:

Address:

Phone:

Fax:

Case Information

Number: Firefox Case

Name:

Synopsis:

Case Time Zone Display

Time Zone: -0:00 UTC Universal (Coordinated) Time

Example: 2017-05-31 12:06:54 (UTC)

Figure 8.1. Case details

2. Now we are ready to add evidence. Click on the green **Add** button in front of **EVIDENCE**. As we have already exported a Firefox profile folder, click on the green **Add** button again, then the **Add folder** button, and choose the folder you exported.

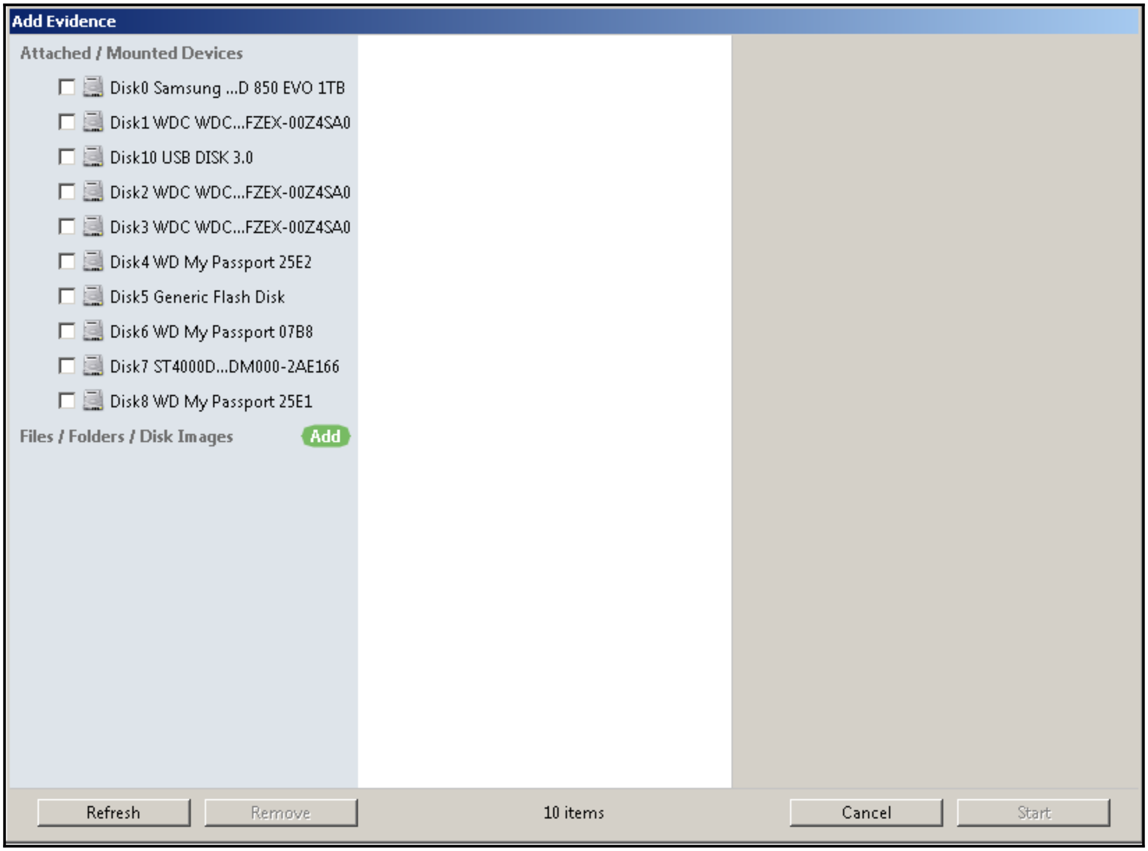
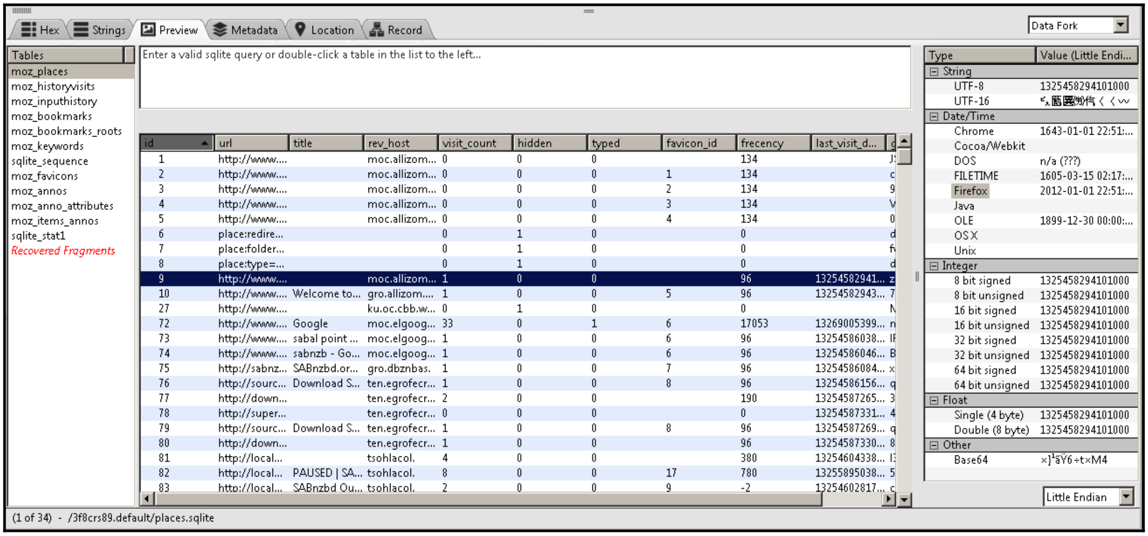

Add Evidence
Attached / Mounted Devices
□ Disk0 Samsung ...D 850 EVO 1TB
□ Disk1 WDC WDC...FZEX-00Z4SA0
□ Disk10 USB DISK 3.0
□ Disk2 WDC WDC...FZEX-00Z4SA0
□ Disk3 WDC WDC...FZEX-00Z4SA0
□ Disk4 WD My Passport 25E2
□ Disk5 Generic Flash Disk
□ Disk6 WD My Passport 07B8
□ Disk7 ST4000D...DM000-2AE166
□ Disk8 WD My Passport 25E1
Files / Folders / Disk Images
Add
Refresh
Remove
10 items
Cancel
Start

Figure 8.2. Adding evidence

3. Once the data has been processed, you should find the extracted data in the **Internet** tab. If, for some reason, this tab does not have the desired contents, you can analyze Firefox SQLite databases manually - BlackLight has a powerful built-in SQLite browser!

Let's use it and analyze `places.sqlite` - an SQLite database that contains information about the suspect's browsing history. Go to the **Browser** tab, choose the database, and use the **Preview** feature to examine it with BlackLight SQLite browser.



Enter a valid sqlite query or double-click a table in the list to the left...

Tables
moz_places
moz_historyvisits
moz_inputhistory
moz_bookmarks
moz_bookmarks_roots
moz_keywords
sqlite_sequence
moz_favicons
moz_annos
moz_anno_attributes
moz_items_annos
sqlite_stat1
Recovered Fragments

id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frecency	last_visit_d...	g
1	http://www....		moc.allizom...	0	0	0		134		J:
2	http://www....		moc.allizom...	0	0	0	1	134		c
3	http://www....		moc.allizom...	0	0	0	2	134		9
4	http://www....		moc.allizom...	0	0	0	3	134		V
5	http://www....		moc.allizom...	0	0	0	4	134		0
6	place:redire...			0	1	0		0		d
7	place:folder...			0	1	0		0		f
8	place:type=...			0	1	0		0		d
9	http://www....		moc.allizom...	1	0	0		96	13254582941...	z
10	http://www....	Welcome to...	gro.allizom....	1	0	0	5	96	13254582943...	7
27	http://www....		ku.oc.cbb.w...	0	1	0		0		N
72	http://www....	Google	moc.elgoog...	33	0	1	6	17053	13269005399...	n
73	http://www....	sabal point ...	moc.elgoog...	1	0	0	6	96	13254586038...	IF
74	http://www....	sabnzb - Go...	moc.elgoog...	1	0	0	6	96	13254586046...	B
75	http://sabnz...	SABnzbd.or...	gro.dbznbas.	1	0	0	7	96	13254586084...	x
76	http://sourc...	Download S...	ten.egrofecr...	1	0	0	8	96	13254586156...	q
77	http://down...		ten.egrofecr...	2	0	0		190	13254587265...	3
78	http://super...		ten.egrofecr...	0	0	0		0	13254587331...	4
79	http://sourc...	Download S...	ten.egrofecr...	1	0	0	8	96	13254587269...	q
80	http://down...		ten.egrofecr...	1	0	0		96	13254587330...	8
81	http://local...		tsohlacol.	4	0	0		380	13254604338...	I3
82	http://local...	PAUSED | SA...	tsohlacol.	8	0	0	17	780	13255895038...	5
83	http://local...	SABnzbd Ou...	tsohlacol.	2	0	0	9	-2	13254602817...	c

(1 of 34) - /3f8crs89.default/places.sqlite

Type	Value (Little Endi...
String	
UTF-8	1325458294101000
UTF-16	ᄃ⅄䨫圄惆く〈〰
Date/Time	
Chrome	1643-01-01 22:51:...
Cocoa/Webkit	
DOS	n/a (???)
FILETIME	1605-03-15 02:17:...
Firefox	2012-01-01 22:51:...
Java	
OLE	1899-12-30 00:00:...
OS X	
Unix	
Integer	
8 bit signed	1325458294101000
8 bit unsigned	1325458294101000
16 bit signed	1325458294101000
16 bit unsigned	1325458294101000
32 bit signed	1325458294101000
32 bit unsigned	1325458294101000
64 bit signed	1325458294101000
64 bit unsigned	1325458294101000
Float	
Single (4 byte)	1325458294101000
Double (8 byte)	1325458294101000
Other	
Base64	×}¹ãŸ6÷t×M4

Figure 8.3. Manual analysis of 'places.sqlite' SQLite database

4. Date/Time feature. Have you noticed the **Recovered Fragments** table? This can help an examiner to recover deleted data - in our case, deleted web history records.

How it works...

BlackLight analyzes Firefox databases and extracts available data (including deleted data) for further examination, including history, bookmarks, downloads, forms data, cookies, and so on. Also, a built-in SQLite browser enables the examiner to analyze these databases manually.

See also

BlackBag BlackLight page: `https://www.blackbagtech.com/blacklight.html`

BlackBag BlackLight Quick Start Guide: `https://www.blackbagtech.com/resources/quickstart-guides/quickstart-guide-blacklight.html`

Google Chrome analysis with Magnet AXIOM

Google Chrome is another very popular web browser. You will find its artifacts during many forensic examinations, not only on Windows systems, but also macOS, Linux, and even mobile platforms. With the help of this recipe you will learn how to parse Google Chrome artifacts with Magnet AXIOM.

Getting ready

Of course, you can use the whole forensic image as the source, but it is much faster to extract the Google Chrome folder from the user's profile, as this greatly reduces the dataset that has to be parsed. Here is where you can find the folders you need:

Windows XP:

```
C:\Documents and Settings\%USERNAME%\Local Settings\Application
Data\Google\Chrome
```

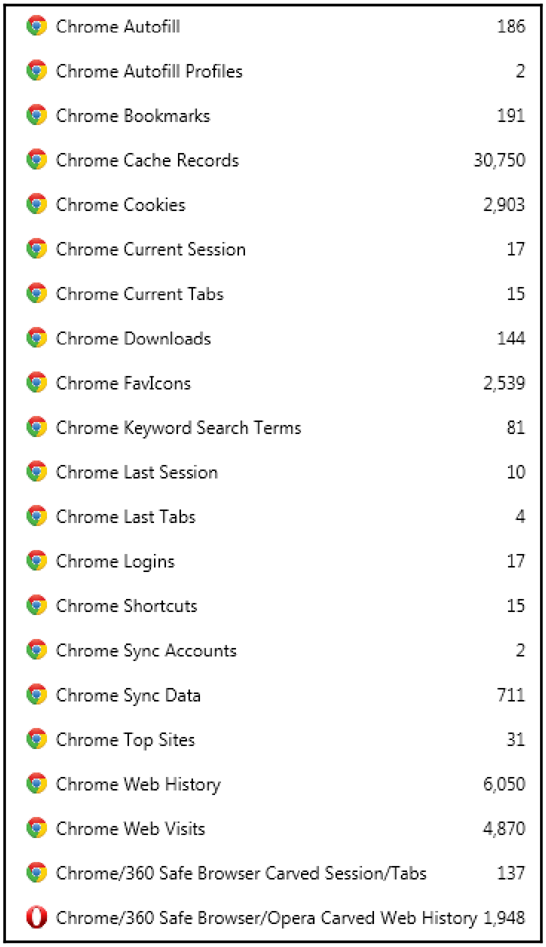
Windows Vista and above:

```
C:\Users\%USERNAME%\AppData\Local\Google\Chrome
```

Export the folder, make sure Magnet AXIOM with a valid licence or trial is installed on your forensic workstation, and you are ready to go.

How to do it...

Create a new case in AXIOM, use the folder you exported as the evidence source, and make sure Google Chrome is chosen in the artifacts list. As soon as all these steps are performed, run evidence analysis. It won't take too much time, but you'll get lots of useful forensic artifacts. The artifacts extracted in our case are shown in the following figure.



Chrome Autofill	186
Chrome Autofill Profiles	2
Chrome Bookmarks	191
Chrome Cache Records	30,750
Chrome Cookies	2,903
Chrome Current Session	17
Chrome Current Tabs	15
Chrome Downloads	144
Chrome FavIcons	2,539
Chrome Keyword Search Terms	81
Chrome Last Session	10
Chrome Last Tabs	4
Chrome Logins	17
Chrome Shortcuts	15
Chrome Sync Accounts	2
Chrome Sync Data	711
Chrome Top Sites	31
Chrome Web History	6,050
Chrome Web Visits	4,870
Chrome/360 Safe Browser Carved Session/Tabs	137
Chrome/360 Safe Browser/Opera Carved Web History	1,948

Figure 8.4. Google Chrome artifacts extracted with Magnet AXIOM

As you can see in the preceding figure, there are quite a lot of artifacts. Let's dive a bit deeper.

- **Chrome Autofill Profiles** are profiles used by Chrome to fill in form fields automatically.
- **Chrome Bookmarks** are webpages bookmarked by the user.
- **Chrome Cache Records** are files downloaded by the browser to speed up the loading of webpages. This can include pictures, HTML, javascript, and so on.
- **Chrome Cookies** - small files which contain information about websites visited by the user.
- **Chrome Current Session** - information about the current session.
- **Chrome Current Tabs** - tabs opened in the current session.
- **Chrome Downloads** - files downloaded with Google Chrome.
- **Chrome FavIcons** - favicons from the Chrome address bar.
- **Chrome Keyword Search Terms** - keywords entered by the user.
- **Chrome Last Session** - information about the previous session.
- **Chrome Last Tabs** - tabs opened in the previous session.
- **Chrome Logins** - the user's login information saved by Chrome.
- **Chrome Shortcuts** - shortcuts for user entered URLs.
- **Chrome Sync Accounts** - user accounts used for syncing to the cloud.
- **Chrome Sync Data** - data synced to the cloud.
- **Chrome Top Sites** - most frequently visited websites.
- **Chrome Web History** - websites the user visited (unique visits only).
- **Chrome Web Visits** - websites the user visited (all visits).

Also, AXIOM uses a carving technique to recover deleted data from Chrome databases.

How it works...

Magnet AXIOM finds and parses Google Chrome artifacts from a forensic image, drive, folder, or file specified by a digital forensic examiner. Parsed artifacts are divided into several groups to make forensicating even more convenient.

See also

Digital Forensics: Artifact Profile – Google Chrome:

```
https://www.magnetforensics.com/artifact-profiles/artifact-profile-google-ch
rome/
```

Microsoft Internet Explorer and Microsoft Edge analysis with Belkasoft Evidence Center

Hopefully, you have already added Belkasoft Evidence Center to your Windows forensic toolkit. As you will remember, it can help you to carve data out of memory dumps. Of course, this is not the only task it can help you to solve. It has robust support for hundreds of Windows operating system forensic artifacts, including different web browsers. In this recipe, we will show you how to use it for Microsoft Internet Explorer and Microsoft Edge forensic analysis.

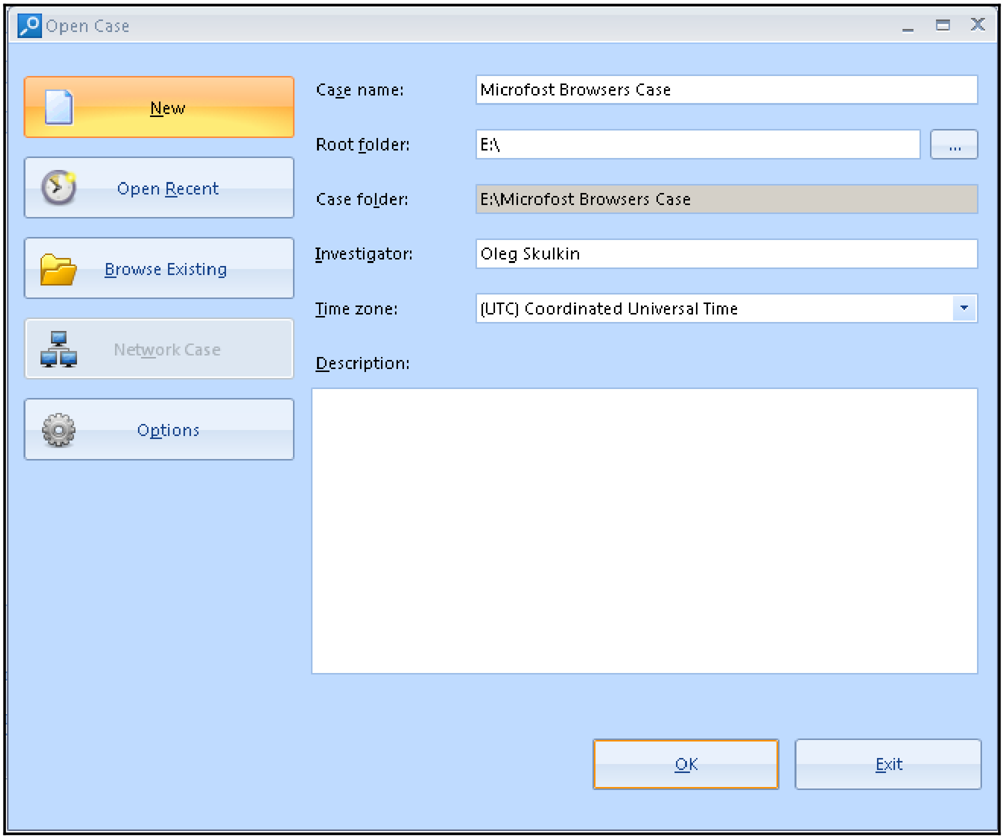
Getting ready

If you already have Belkasoft Evidence Center installed, just start the tool. Otherwise, use the trial download link from the *See also* section to obtain a trial version of the tool. You will need a Windows 10 image, as we are planning to analyze Microsoft Edge data.

How to do it...

The steps for Microsoft Edge analysis and Microsoft Internet Explorer Analysis using Belkasoft Evidence Center are as follows:

1. First of all, let's create a new case. Fill in the case information, choose the **Root folder** (the case folder will be created automatically), and don't forget to make sure you choose the right time zone from the drop-down menu. If you want, you can add a case description as well.



Case name: Microfost Browsers Case

Root folder: E:\

Case folder: E:\Microfost Browsers Case

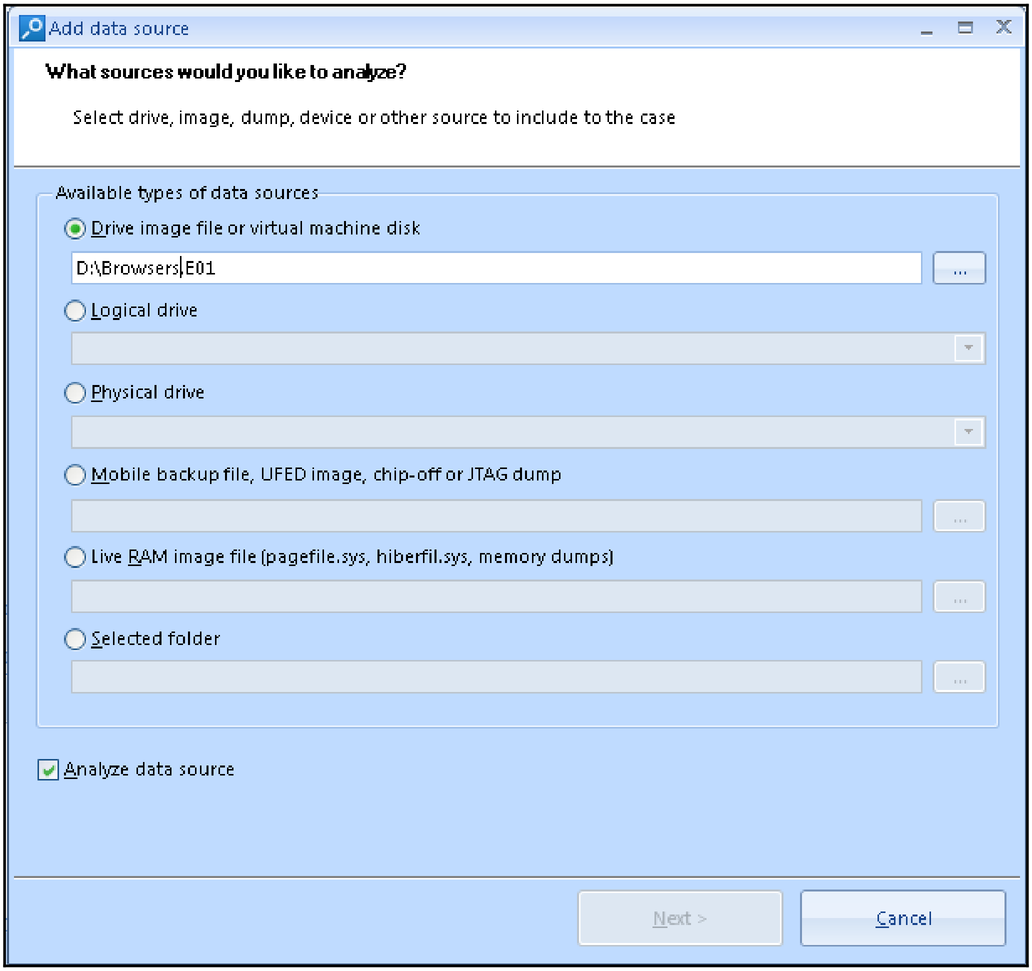
Investigator: Oleg Skulkin

Time zone: (UTC) Coordinated Universal Time

Description:

Figure 8.5. Creating a new case in Belkasoft Evidence Center

2. Now it's time to choose a data source. As you can see in the following figure, we have a number of options here. This time, we are going to choose a drive image. We have a test image named `Browsers.E01`. If you have created an image of a Windows 10 drive, you can use it for this recipe, otherwise, find such a system and solidify your knowledge by imaging it. Also, you can create a Windows 10 virtual machine and use its virtual disk - such disks are also supported by Belkasoft Evidence Center.



Add data source

What sources would you like to analyze?

Select drive, image, dump, device or other source to include to the case

Available types of data sources

● Drive image file or virtual machine disk

D:\Browsers.E01

○ Logical drive

○ Physical drive

○ Mobile backup file, UFED image, chip-off or JTAG dump

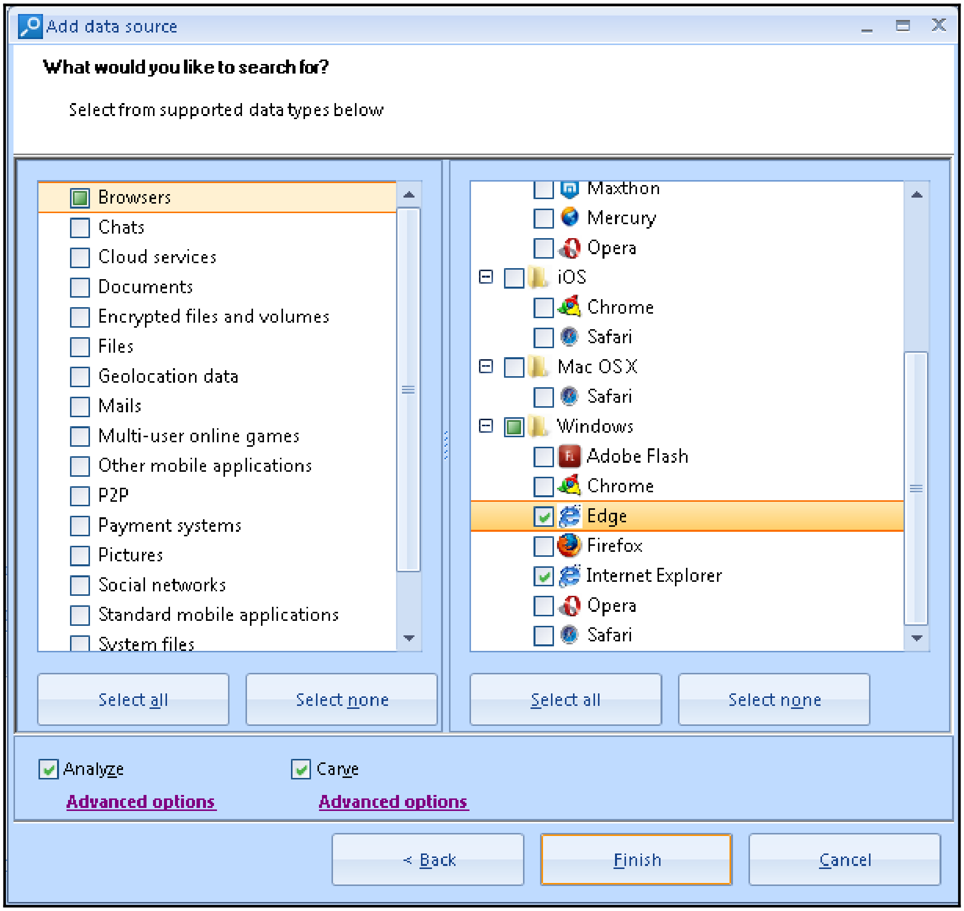
○ Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

○ Selected folder

☑ Analyze data source

Figure 8.6. Adding a data source in Belkasoft Evidence Center

3. Let's choose the forensic artifacts we want to search for. First, click on the **Select none** to uncheck all data types. Now go to **Browsers**, scroll down to **Windows** on the left pane, and choose **Edge,** and then **Internet Explorer**. Don't forget to tick the **Carve** option to extract even more data!



Add data source

What would you like to search for?

Select from supported data types below

- ■ Browsers
- □ Chats
- □ Cloud services
- □ Documents
- □ Encrypted files and volumes
- □ Files
- □ Geolocation data
- □ Mails
- □ Multi-user online games
- □ Other mobile applications
- □ P2P
- □ Payment systems
- □ Pictures
- □ Social networks
- □ Standard mobile applications
- □ System files

- □ Maxthon
- □ Mercury
- □ Opera
- ⊟ □ iOS
  - □ Chrome
  - □ Safari
- ⊟ □ Mac OS X
  - □ Safari
- ⊟ ■ Windows
  - □ Adobe Flash
  - □ Chrome
  - ☑ Edge
  - □ Firefox
  - ☑ Internet Explorer
  - □ Opera
  - □ Safari

☑ Analyze ☑ Carve

Figure 8.7. Choosing data types in Belkasoft Evidence Center

Once the image has been processed, you'll see all the results in both the **Overview** and **Case Explorer** tabs.

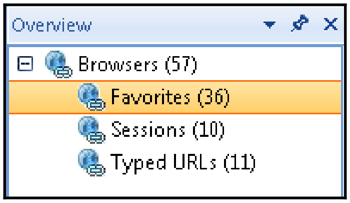


Figure 8.8. Overview tab

4. If you dig deeper and analyze browser history artifacts, you will notice that all of them are marked as **Internet Explorer 10+**. This is because both Internet Explorer and Edge store history records in the same database, located at: `C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat`

   Also, you can see the **Typed URLs** section in the preceding figure. These URLs are typed by the user directly into the browser's address bar, and are stored in the registry. You can learn more about Windows Registry forensics in `Chapter 6`, *Windows Registry Analysis*.

How it works...

Belkasoft Evidence Center walks through all files and folders and extracts available data from web browsers. If carving is enabled, it also extracts data from unallocated space.

See also

Belkasoft Evidence Center download page:

`https://belkasoft.com/get`

Internet Explorer developer documentation:

`https://msdn.microsoft.com/en-us/library/hh772401(v=vs.85).aspx`

Microsoft Edge developer documentation:

`https://docs.microsoft.com/en-us/microsoft-edge/`

Extracting web browser data from Pagefile.sys

You already know that you can extract quite a lot of useful forensic artifacts from a memory dump. But there is more: you can perform memory forensics even without a memory dump! There are files on the drive that contain some parts of memory. These files are `pagefile.sys`, `swapfile.sys`, and `hiberfil.sys`, and they are located at the system root (`C:\`). In this recipe, we will show you how to extract browser data from `pagefile.sys` with Belkasoft Evidence Center.

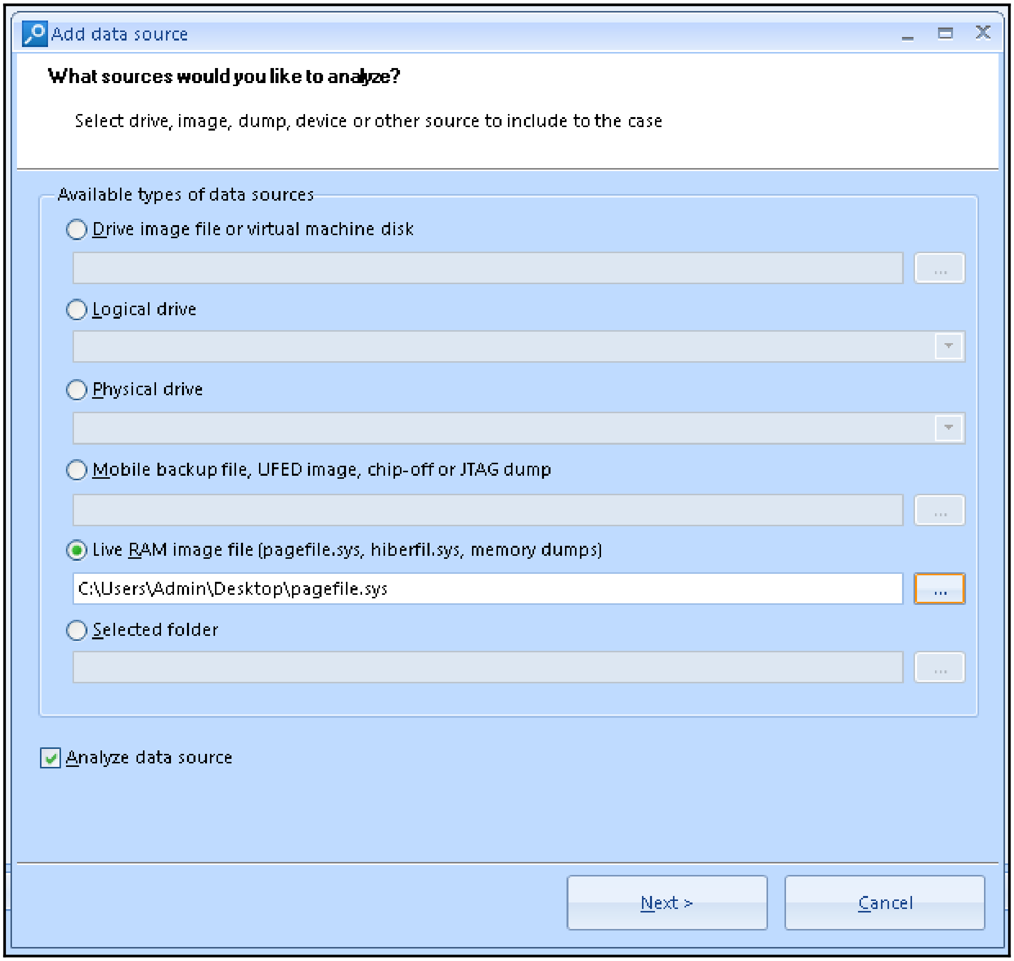
Getting ready

First of all, make sure you have Belkasoft Evidence Center with a valid licence (or a trial version) installed on your workstation. Then, use a tool of your choice, for example FTK Imager, to export data from your own system or from a forensic image you acquired earlier. As soon as you have this, you are ready to go.

How to do it...

The steps to extract web browser data from `Pagefile.sys` are as follows:

1. Start by creating a new case in Belkasoft Evidence Center - you already know how to do this. Then, add the `pagefile.sys` file you exported previously as the evidence source.



Add data source

What sources would you like to analyze?

Select drive, image, dump, device or other source to include to the case

Available types of data sources

○ Drive image file or virtual machine disk

○ Logical drive

○ Physical drive

○ Mobile backup file, UFED image, chip-off or JTAG dump

● Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

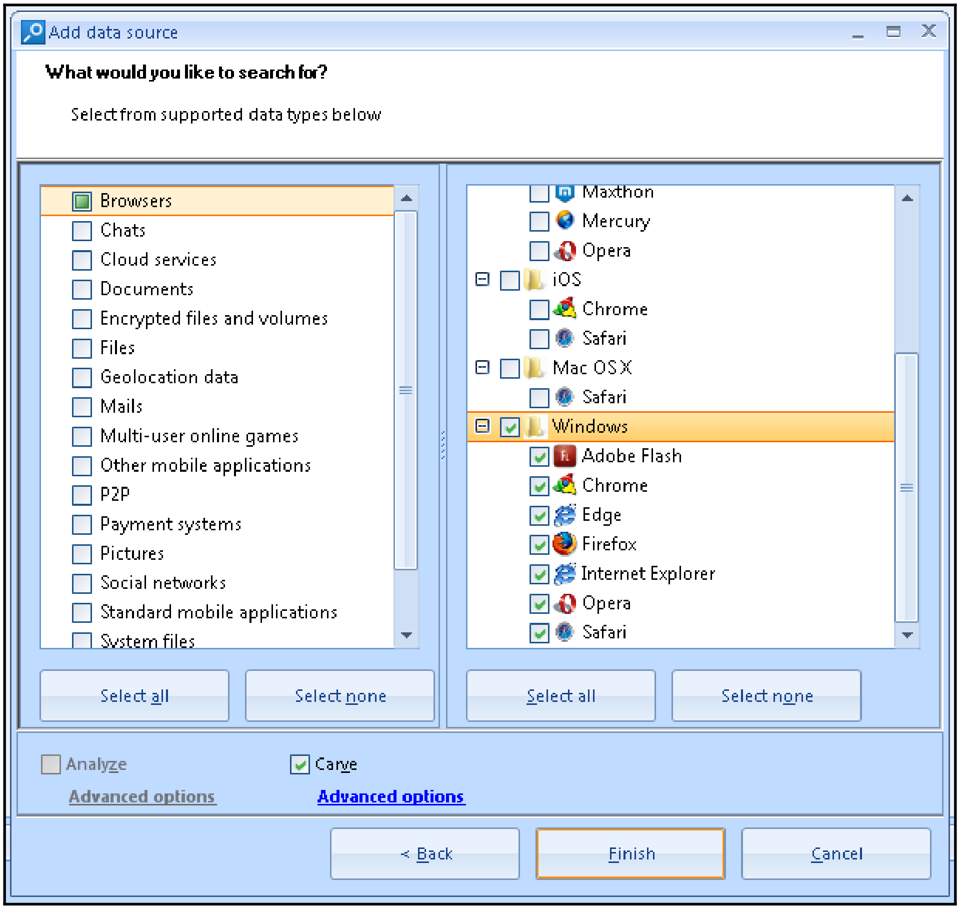
C:\Users\Admin\Desktop\pagefile.sys

○ Selected folder

☑ Analyze data source

Figure 8.9. Adding pagefile.sys as the evidence source

2. As we are planning to extract web browser artifacts and are dealing with a Windows system, let's choose corresponding data types, as in the following figure:



Add data source

What would you like to search for?

Select from supported data types below

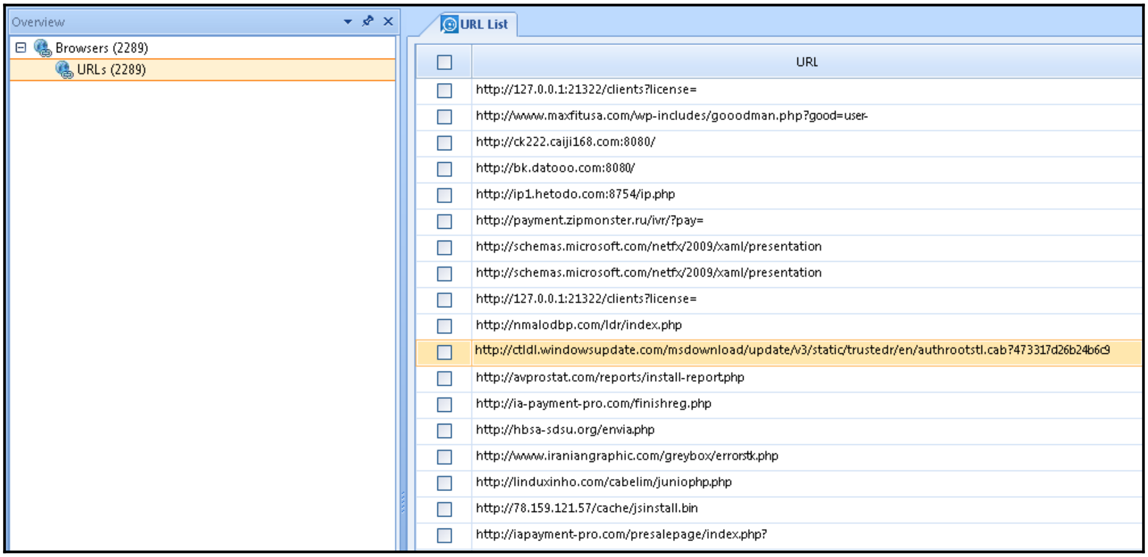
- ▣ Browsers
- □ Chats
- □ Cloud services
- □ Documents
- □ Encrypted files and volumes
- □ Files
- □ Geolocation data
- □ Mails
- □ Multi-user online games
- □ Other mobile applications
- □ P2P
- □ Payment systems
- □ Pictures
- □ Social networks
- □ Standard mobile applications
- □ System files

- □ Maxthon
- □ Mercury
- □ Opera
- □ iOS
  - □ Chrome
  - □ Safari
- □ Mac OS X
  - □ Safari
- ☑ Windows
  - ☑ Adobe Flash
  - ☑ Chrome
  - ☑ Edge
  - ☑ Firefox
  - ☑ Internet Explorer
  - ☑ Opera
  - ☑ Safari

□ Analyze ☑ Carve

Figure 8.10. Choosing data types

3. Click **Finish** and the processing will start. Once the processing phase has finished, go to the **Overview** tab and check the results.



□	URL
□	http://127.0.0.1:21322/clients?license=
□	http://www.maxfitusa.com/wp-includes/gooodman.php?good=user-
□	http://ck222.caiji168.com:8080/
□	http://bk.datooo.com:8080/
□	http://ip1.hetodo.com:8754/ip.php
□	http://payment.zipmonster.ru/ivr/?pay=
□	http://schemas.microsoft.com/netfx/2009/xaml/presentation
□	http://schemas.microsoft.com/netfx/2009/xaml/presentation
□	http://127.0.0.1:21322/clients?license=
□	http://nmalodbp.com/ldr/index.php
□	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?473317d26b24b6c9
□	http://avprostat.com/reports/install-report.php
□	http://ia-payment-pro.com/finishreg.php
□	http://hbsa-sdsu.org/envia.php
□	http://www.iraniangraphic.com/greybox/errorstk.php
□	http://linduxinho.com/cabelim/juniophp.php
□	http://78.159.121.57/cache/jsinstall.bin
□	http://iapayment-pro.com/presalepage/index.php?

Figure 8.11. Processing results

As you can see in the preceding figure, we have 2289 URLs extracted from pagefile.sys! Impressive, isn't it? You can do the same with two other files: swapfile.sys and hiberfil.sys.

How it works...

Belkasoft Evidence Center walks through `Pagefile.sys` and extracts records from available web browsers. If a digital forensic examiner chooses more data types, it can extract even more data, including images, messages, emails, and so on.

See also

What is the Page File for anyway?

https://blogs.technet.microsoft.com/askperf/2007/12/14/what-is-the-page-file-for-anyway/

Analyzing hibernation and page files:

http://ru.belkasoft.com/ru/bec/en/Hibernation_And_Page_Files_Investigation.asp

9
Email and Instant Messaging Forensics

In this chapter, we will cover the following recipes:

- Outlook mailbox parsing with Intella
- Thunderbird mailbox parsing with Autopsy
- Webmail analysis with Magnet AXIOM
- Skype forensics with Belkasoft Evidence Center
- Skype forensics with SkypeLogView

Introduction

Accessing a suspect's communications via email and instant messengers will help you to solve lots of cases; and you will be asked to find and extract such artifacts very often. It doesn't matter if the case is a phishing attack, intellectual property theft, or a terrorist act - a computer forensic examiner must be able to locate, parse, and analyze a suspect's digital communications.

In this chapter, we will show you how to parse and analyze artifacts from the most common Windows email clients - Microsoft Outlook, Mozilla Thunderbird, and Skype instant messenger.

Outlook mailbox parsing with Intella

Intella is a very powerful digital forensic and eDiscovery tool capable of processing, searching, and analyzing **Electronically Stored Information** (**ESI**). One of its main features is visual analytics. This feature can help an examiner to understand the ESI and custodian relationships better. In this recipe, we will show you how to parse an Outlook mailbox with this tool.

Getting ready

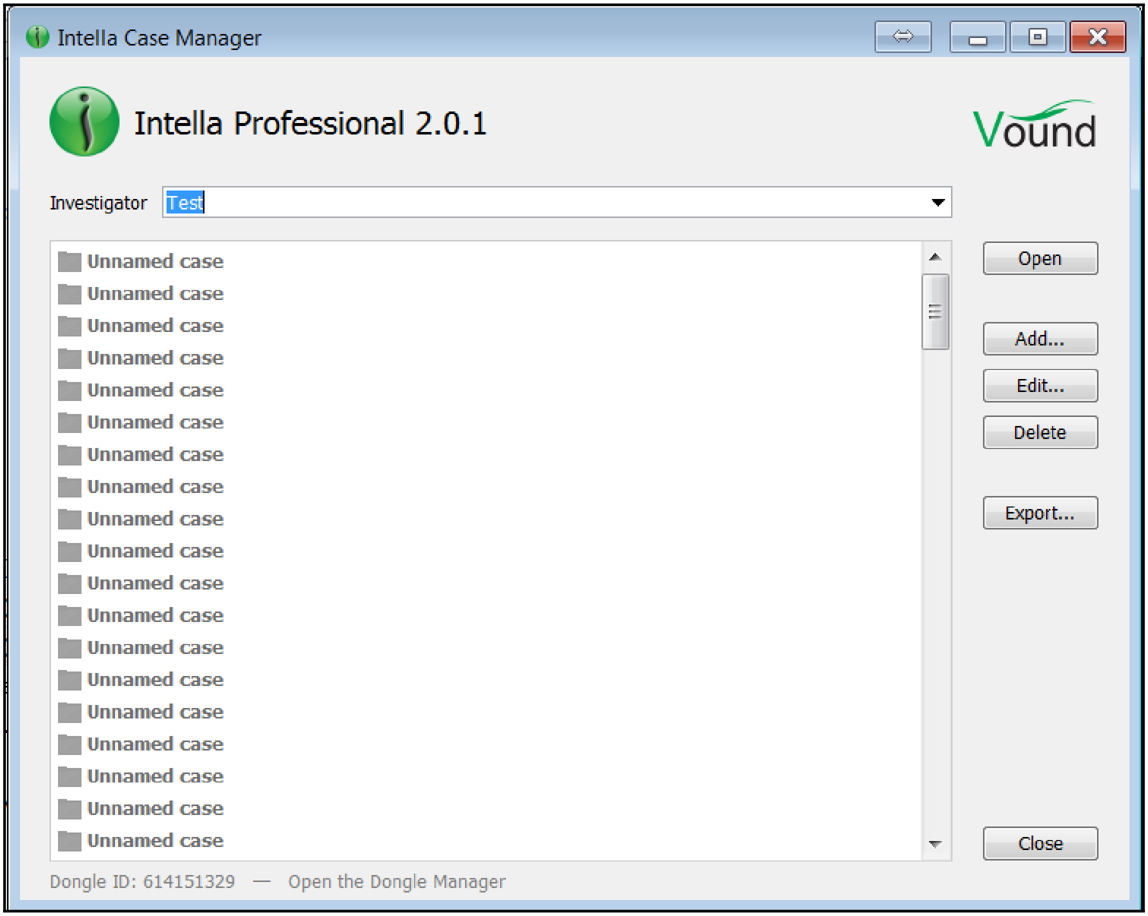
If you don't have a valid Intella license, you can get a free 14-day trial version from Vound Software's website (check the *See also* section). You will also need a `PST` or `OST` file to follow this recipe. It's easy to get one: simply use your own email address with Outlook, then go to `C:\Users\%USERNAME%\AppData\Local\Microsoft\Outlook` and get your file. This will be your evidence source, in our case an `OST` file.

PST files are used for POP3, IMAP, and web-based mail accounts, while OST files are used when a user has an Exchange account and wants to work offline.

How to do it...

We can start the process by following the given steps:

1. Start by creating a new case. To do this, run Intella (you'll see Intella Case Manager), type your name (in our case it's `Test`), and click the **Add...** button, as shown in the following figure:



Intella Case Manager

Intella Professional 2.0.1

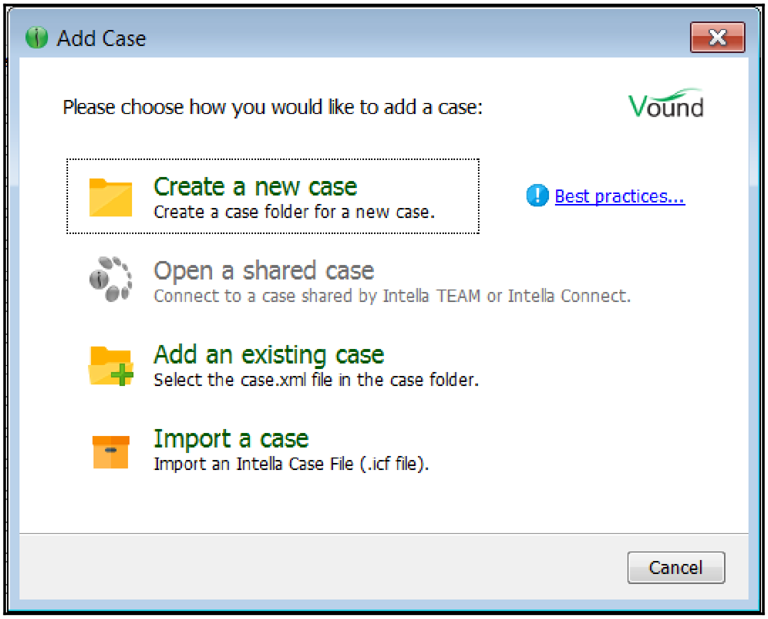
Investigator: Test

Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case
Unnamed case

Dongle ID: 614151329 — Open the Dongle Manager

Figure 9.1. Adding a new case

2. Using the **Add Case** dialog, an examiner can **Create a new case**, **Open a shared case**, **Add an existing case,** or **Import a case**.



Add Case

Please choose how you would like to add a case:

Create a new case
Create a case folder for a new case.

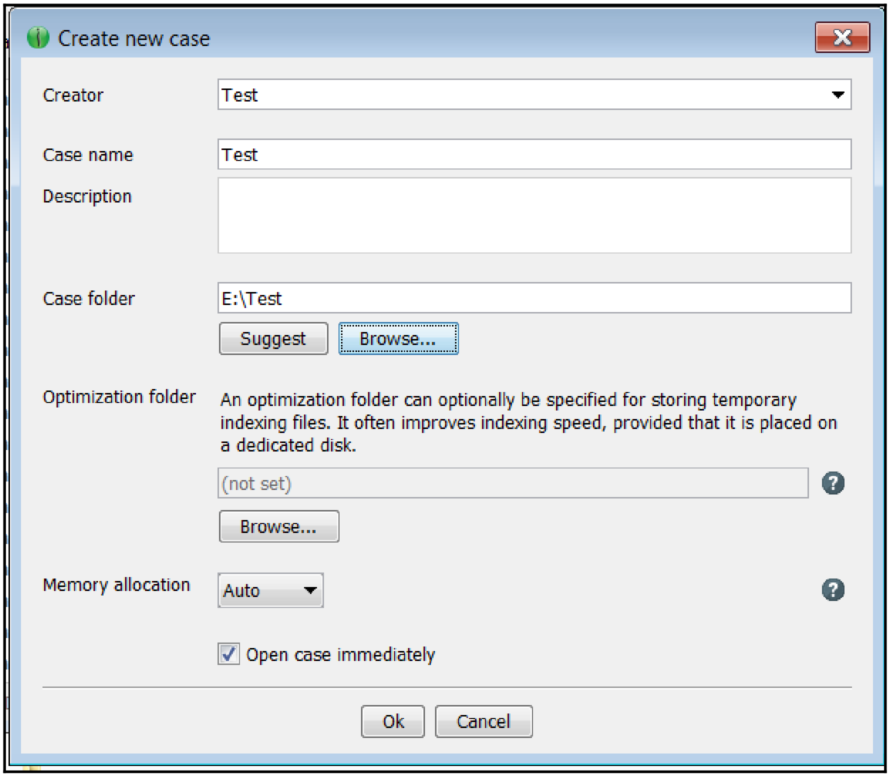
Open a shared case
Connect to a case shared by Intella TEAM or Intella Connect.

Add an existing case
Select the case.xml file in the case folder.

Import a case
Import an Intella Case File (.icf file).

Figure 9.2. Add Case dialog

3. As we have decided to create a new case, let's choose **Create a new case**. Now you can see a few fields to fill in. Also you can choose a folder for storing the temporary indexing files - it improves the indexing speed!



Creator: Test

Case name: Test

Description:

Case folder: E:\Test

Optimization folder: An optimization folder can optionally be specified for storing temporary indexing files. It often improves indexing speed, provided that it is placed on a dedicated disk.

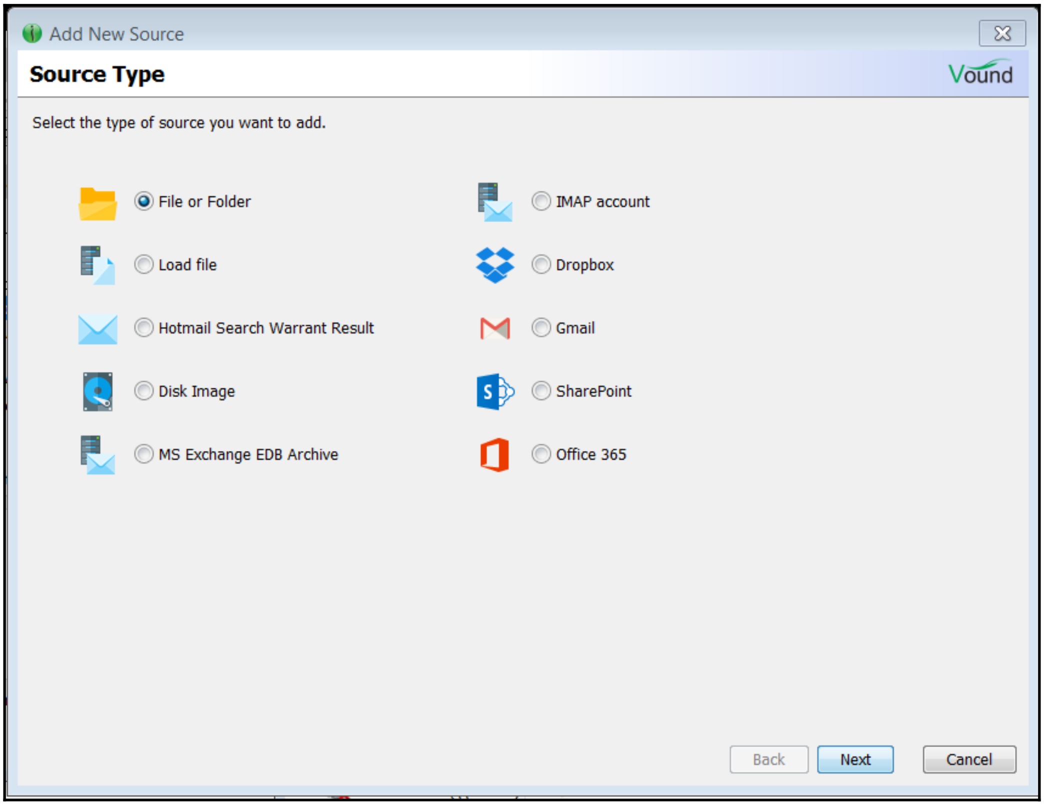
(not set)

Memory allocation: Auto

☑ Open case immediately

Figure 9.3. Creating a new case

4. It's time to choose our evidence source. As we already mentioned, we are going to use an `OST` file, so let's choose the **File or Folder** option, as shown in the following figure:



Add New Source

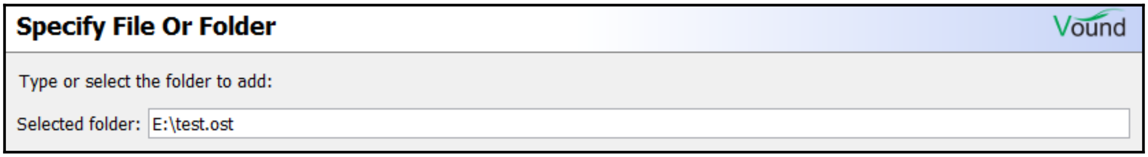
Source Type

Select the type of source you want to add.

● File or Folder	○ IMAP account
○ Load file	○ Dropbox
○ Hotmail Search Warrant Result	○ Gmail
○ Disk Image	○ SharePoint
○ MS Exchange EDB Archive	○ Office 365

Figure 9.4. Adding a new source

5. In our case, the file is named `test.ost` and is located in the root of `E:\ drive`, as you can see in the following figure:



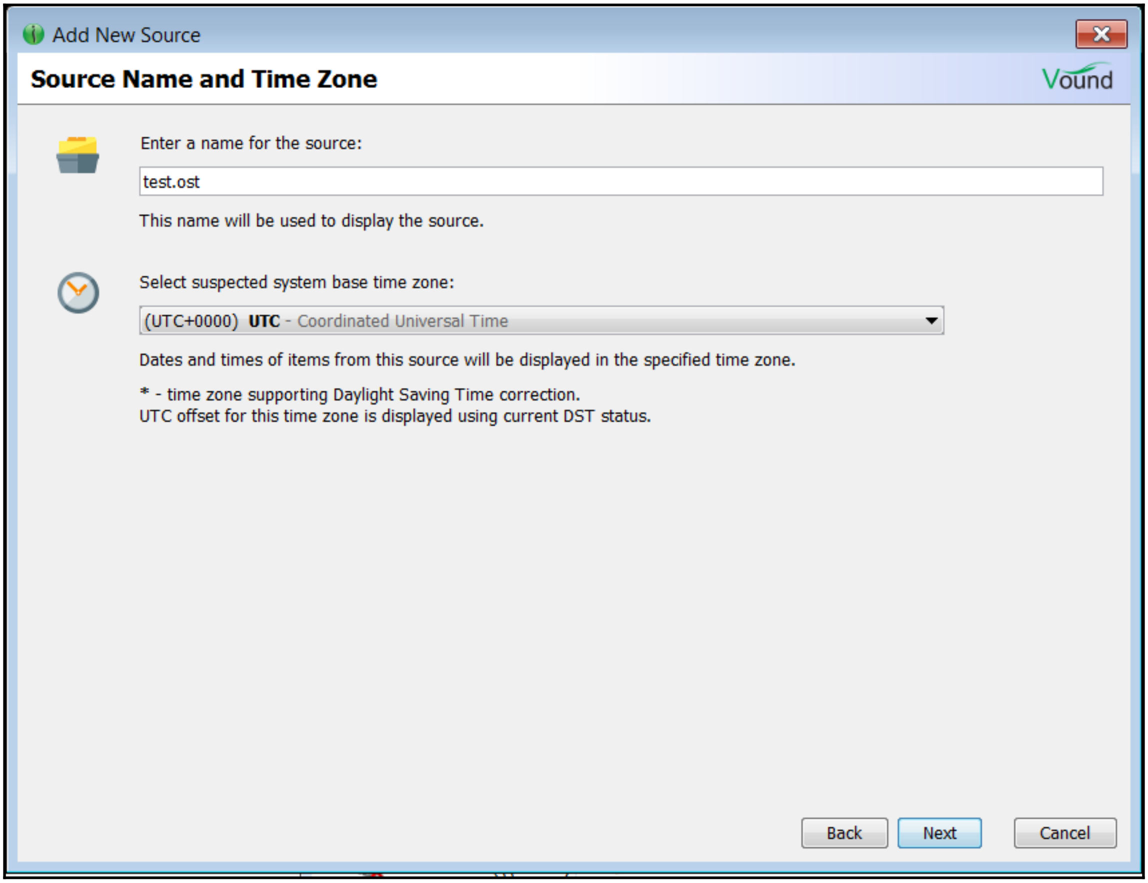
Specify File Or Folder

Type or select the folder to add:

Selected folder: E:\test.ost

Figure 9.5. Adding a file to process

6. If you don't like the original name of the source, you can change it to one you like. Also, you should choose the right time zone, or just choose UTC if the right time zone is unknown.



Source Name and Time Zone

Enter a name for the source:

test.ost

This name will be used to display the source.

Select suspected system base time zone:

(UTC+0000) **UTC** - Coordinated Universal Time

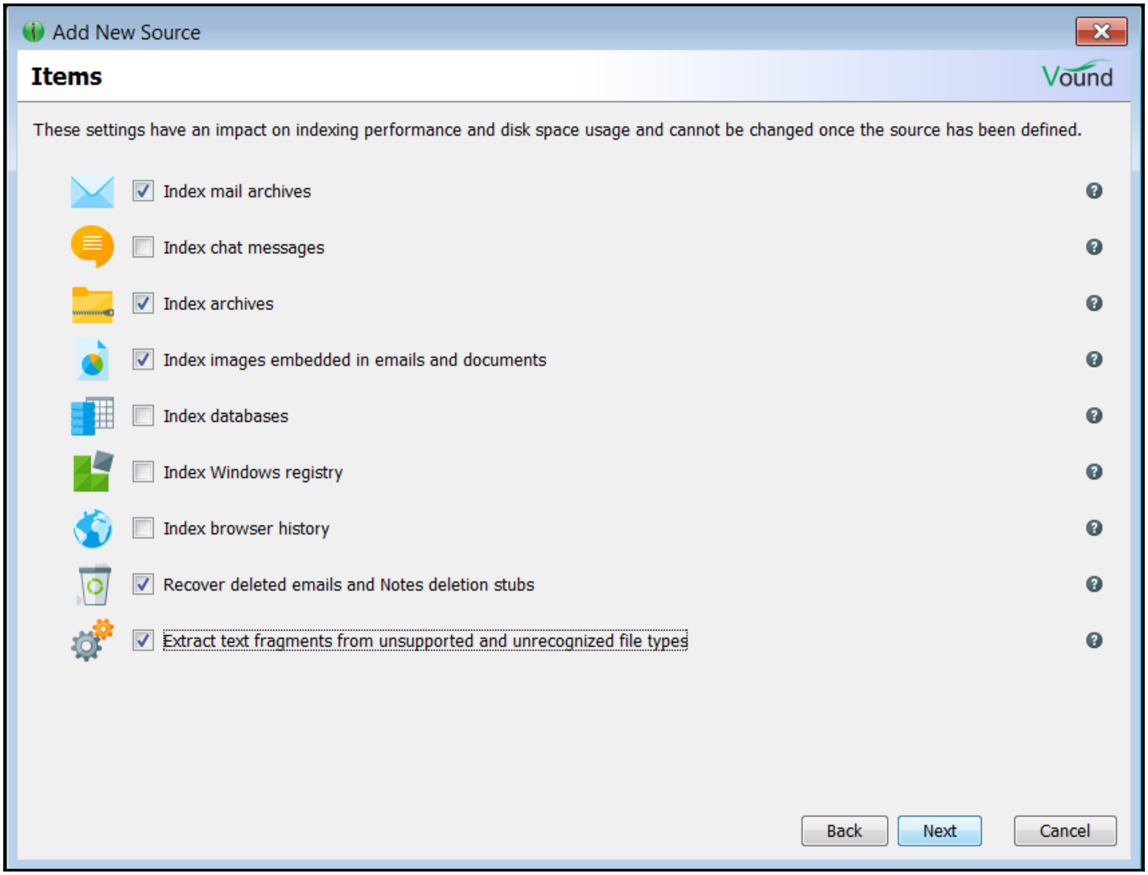
Dates and times of items from this source will be displayed in the specified time zone.

* - time zone supporting Daylight Saving Time correction.
UTC offset for this time zone is displayed using current DST status.

Figure 9.6. Choosing the source name and the time zone

7. OK, let's choose the items we want to process. In our case, they are the following:
    - Mail archives: we are processing an Outlook mailbox, so this is very important
    - Archives: can be attached to emails
    - Images embedded in emails and documents

- Deleted emails
- Text fragments from unsupported and unrecognized file types



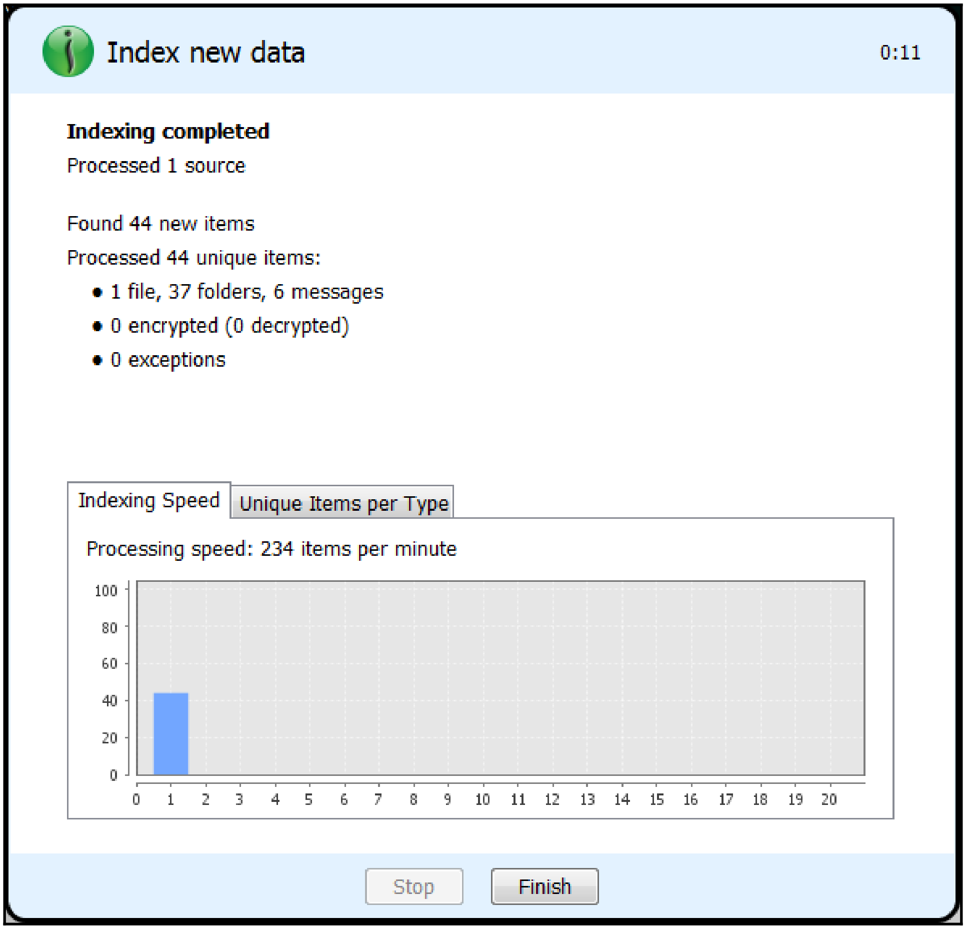
Items

These settings have an impact on indexing performance and disk space usage and cannot be changed once the source has been defined.

- ☑ Index mail archives
- □ Index chat messages
- ☑ Index archives
- ☑ Index images embedded in emails and documents
- □ Index databases
- □ Index Windows registry
- □ Index browser history
- ☑ Recover deleted emails and Notes deletion stubs
- ☑ Extract text fragments from unsupported and unrecognized file types

Figure 9.7. Choosing items to process

8. You can skip two next windows and start evidence processing. Once indexing is complete, you will see the overview, as shown in the following figure:



Indexing completed

Processed 1 source

Found 44 new items

Processed 44 unique items:

- 1 file, 37 folders, 6 messages
- 0 encrypted (0 decrypted)
- 0 exceptions

Processing speed: 234 items per minute

Figure 9.8. Indexing the evidence source

9. Click **Finish** and you'll see the main window with three tabs; look at the following figure:

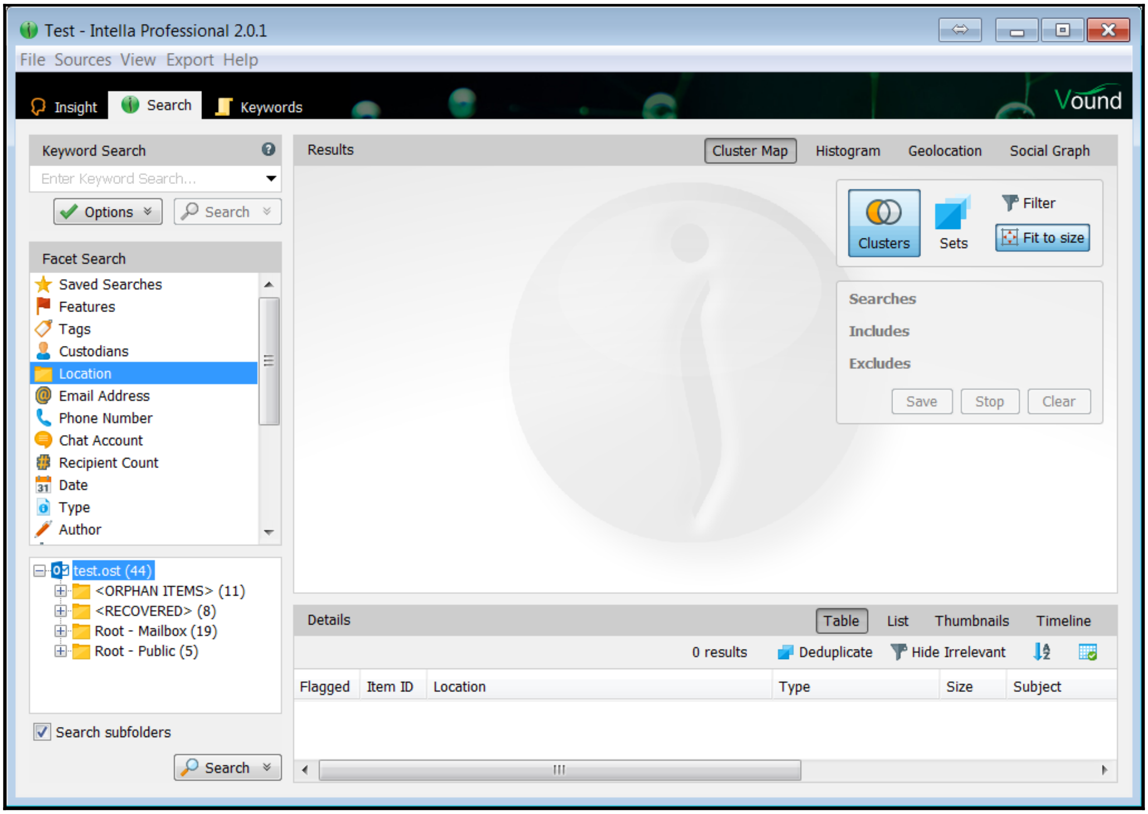
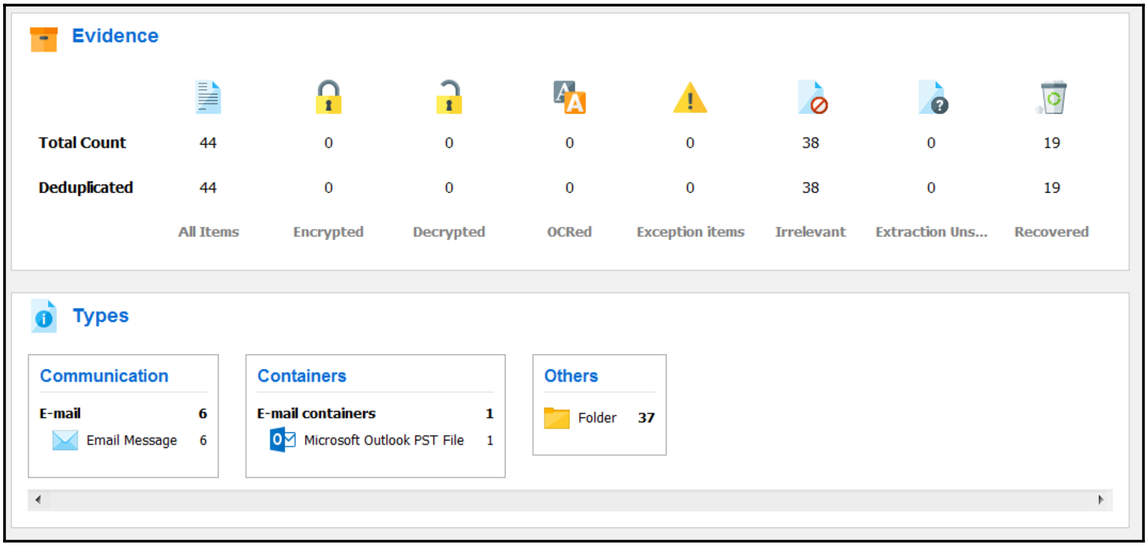


Figure 9.9. Intella Search tab

10. As you can see, we have 44 items, including the 19 that were recovered. Now we can search the indexed data using different keywords and facets, such as email addresses, phone numbers, author, date, type, and so on. Also, we can use this tab to create cluster maps, histograms, and social graphs, which can be very useful.
11. OK, let's go to the **Insight** tab, as shown in the following figure:



Evidence

	All Items	Encrypted	Decrypted	OCRed	Exception items	Irrelevant	Extraction Uns...	Recovered
Total Count	44	0	0	0	0	38	0	19
Deduplicated	44	0	0	0	0	38	0	19

Types

Communication

E-mail	**6**
Email Message	6

Containers

E-mail containers	**1**
Microsoft Outlook PST File	1

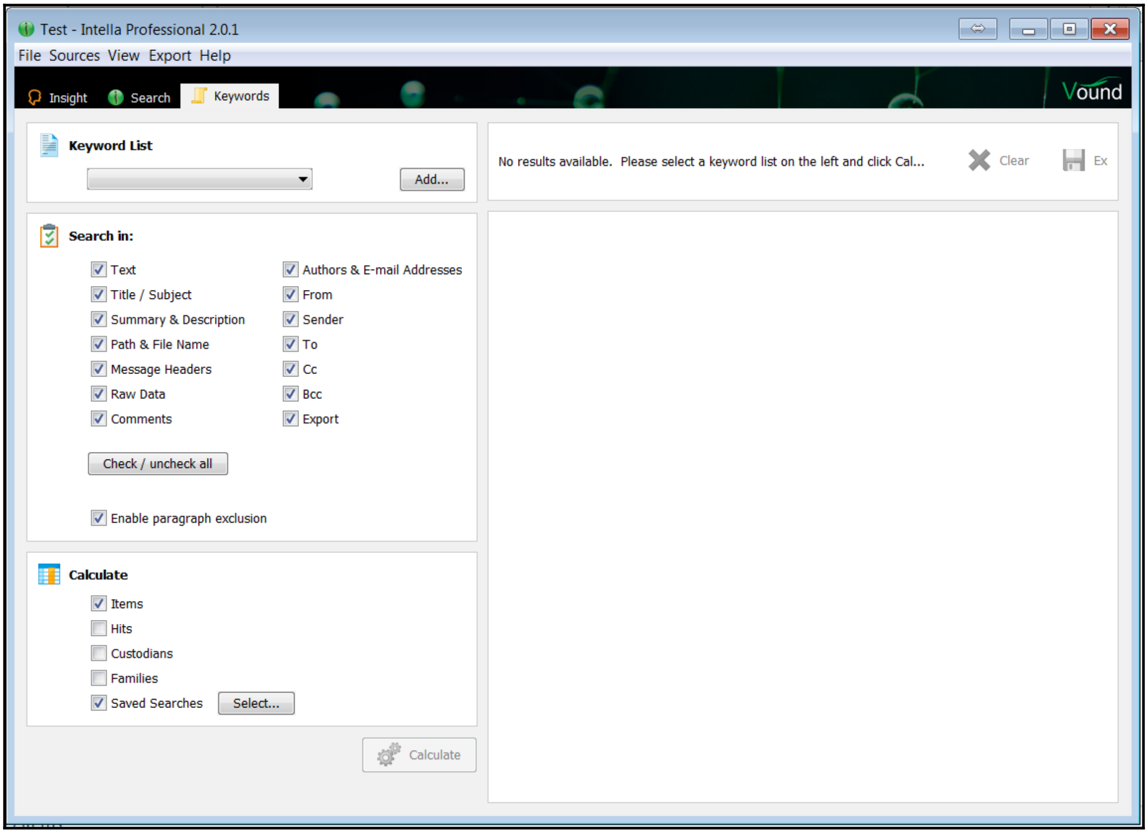
Others

Folder	**37**

Figure 9.10. Intella Insight tab

Here we have the evidence overview. For example, Intella shows us that we are dealing with Microsoft Outlook, we have 19 recovered artifacts, six email messages, and 44 items in total.

12. Let's check the last tab - **Keywords**. Look at the following figure:



No results available. Please select a keyword list on the left and click Cal...

Search in:

- ☑ Text
- ☑ Title / Subject
- ☑ Summary & Description
- ☑ Path & File Name
- ☑ Message Headers
- ☑ Raw Data
- ☑ Comments
- ☑ Authors & E-mail Addresses
- ☑ From
- ☑ Sender
- ☑ To
- ☑ Cc
- ☑ Bcc
- ☑ Export

☑ Enable paragraph exclusion

Calculate

- ☑ Items
- ☐ Hits
- ☐ Custodians
- ☐ Families
- ☑ Saved Searches

Figure 9.11. Intella Keywords tab

First of all, you can use this tab to add custom keyword lists - it can save you time! Also, you can choose where you want to search. For example, if you want to look for keywords only in the emails' subjects, then you can uncheck all options first and choose only 'Title/Subject'.

How it works...

Intella indexes the chosen evidence source and enables a computer forensic examiner to search through the indexed data. It can also be used to create cluster maps, histograms, social graphs, and so on.

See also

Intella overview:

```
https://www.vound-software.com/individual-solutions
```

Introduction to Outlook Data Files (`.pst` and `.ost`):

```
https://support.office.com/en-us/article/Introduction-to-Outlook-Data-Files-
pst-and-ost-6d4197ec-1304-4b81-a17d-66d4eef30b78
```

Thunderbird mailbox parsing with Autopsy

Thunderbird is a free and open source mail client from Mozilla, the developers of the Firefox browser. If a user doesn't use Outlook, they are likely to use Thunderbird. In this recipe, we will show you how to extract data from Thunderbird MBOX files with a free and open source digital forensics platform — **Autopsy**.

Getting ready

Thunderbird stores mail data in MBOX files. These files can be found at the following location:

```
C:\Users\%USERNAME%\AppData\Roaming\Thunderbird\Profiles
```

Here you will find a user profile folder, which can be exported and processed with a piece of forensic software, in our case Autopsy.

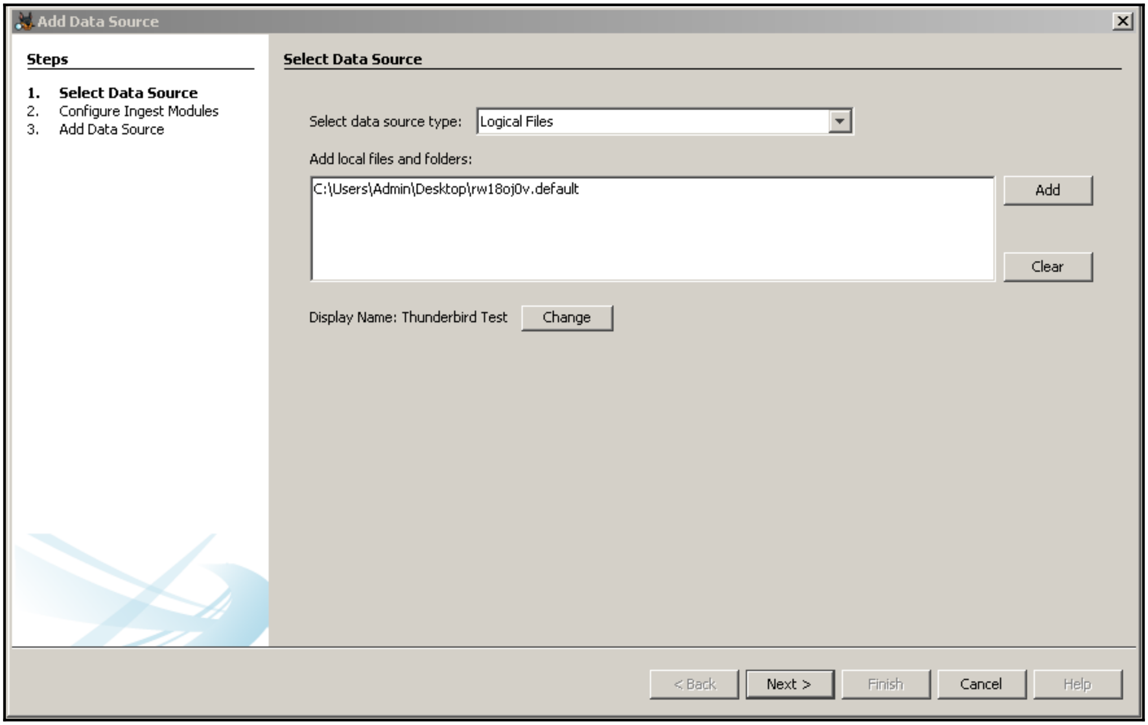
Of course, you can use the whole forensic image for processing, but if you use only the profile folder, it saves you a lot of time.

Get a Thunderbird profile folder or a forensic image, and start Autopsy. If you haven't installed it already, use the download link in the 'See also' section.

How to do it...

We can start the process by following the given steps:

1. Start by creating a new case and filling in the case details. We are planning to use a Thunderbird profile folder as the source, so in the **Select Data Source** window, we choose **Logical Files**.



Select data source type: Logical Files

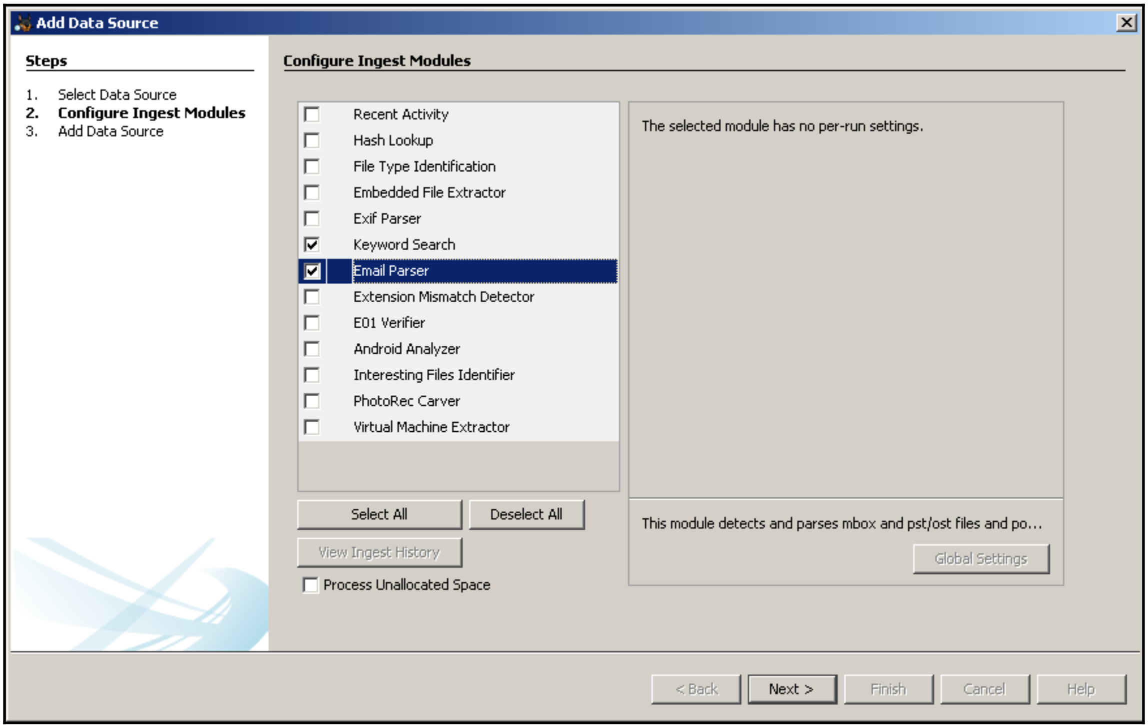
Add local files and folders: C:\Users\Admin\Desktop\rw18oj0v.default

Display Name: Thunderbird Test

Figure 9.12. Selecting data source in Autopsy

Also, you can choose the display name for your evidence source. You will notice that we have named it **Thunderbird Test**.

2. It's time to choose Ingest Modules. We highly recommend always choosing the **Keyword Search** module, as this is very helpful. Of course, this time make sure **Email Parser** is ticked.



□ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Embedded File Extractor
□ Exif Parser
☑ Keyword Search
☑ Email Parser
□ Extension Mismatch Detector
□ E01 Verifier
□ Android Analyzer
□ Interesting Files Identifier
□ PhotoRec Carver
□ Virtual Machine Extractor

□ Process Unallocated Space

The selected module has no per-run settings.

This module detects and parses mbox and pst/ost files and po...

Figure 9.13. Configuring ingest modules in Autopsy

3. Once your data source is processed, you can analyze the results. You can find these in the **Email Messages** section on the left, as shown in the following figure:

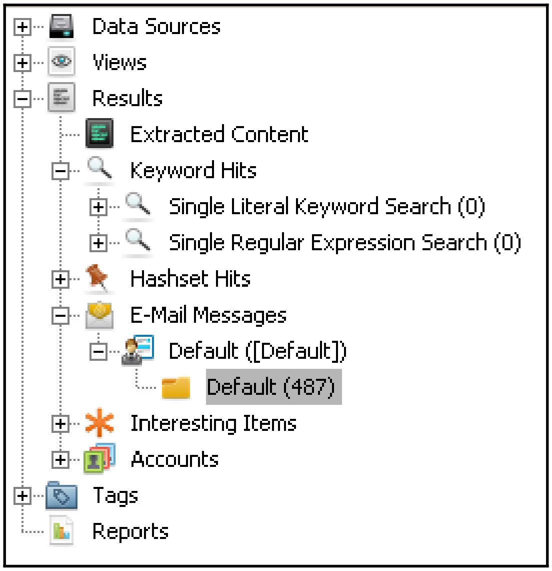


Figure 9.14. Parsed email messages

4. As you can see, there are 487 email messages extracted by Autopsy. On the right, you can find everything you need for analysis: sender, recipient, message body, timestamps, and so on.

How it works...

Autopsy processes the data source specified by a computer forensic examiner and extracts the email data from supported containers, such as MBOX and PST.

See also

Autopsy download page:

`http://sleuthkit.org/autopsy/download.php`

MBOX Email Format:

`https://www.loc.gov/preservation/digital/formats/fdd/fdd000383.shtml`

Webmail analysis with Magnet AXIOM

As you may know, some people (including the authors) use only webmail and no mail clients. Is it possible to recover such forensic artifacts from a drive image? The answer is - yes! And in this recipe, we will show you how to recover webmail activity with Oleg's favorite digital forensic tool - Magnet AXIOM.

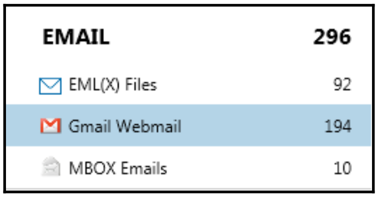
Getting ready

We are sure that you already have AXIOM installed on your workstation. So run the tool and create a new case. Now, the most interesting thing is the evidence source. If you have already walked through the recipe *Extracting Web Browser Data from Pagefile.sys* in `Chapter 8`, *Web Browser Forensics,* you may guess what we are going to do next. Yes, webmail artifacts can be extracted from `pagefile.sys`, `swapfile.sys` and `hiberfil.sys`. So you can use one of these files as the data source, or the whole forensic image - AXIOM will find and parse data from these files automatically.

How to do it...

We can start the process by following the given steps:

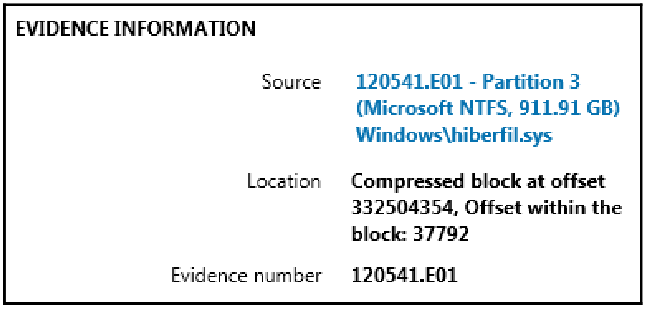
1. Process your data source with AXIOM Process; don't forget to include `pagefile.sys` and `hiberfil.sys`, and make sure mail artifacts are checked. Once the processing phase is finished, go to AXIOM Examine and look at the **EMAIL** section. Here you will find extracted email artifacts, including webmail, in our case Gmail, as shown in the following figure:



EMAIL	296
EML(X) Files	92
Gmail Webmail	194
MBOX Emails	10

Figure 9.15. Extracted webmail artifacts

2. As you can see, 194 Gmail Webmail artifacts have been extracted. Let's check the source of these artifacts, the first artifact in particular. Click on the artifact and check the **EVIDENCE INFORMATION** section.



EVIDENCE INFORMATION

Source	120541.E01 - Partition 3 (Microsoft NTFS, 911.91 GB) Windows\hiberfil.sys
Location	Compressed block at offset 332504354, Offset within the block: 37792
Evidence number	120541.E01

Figure 9.16. Artifact information

Look at the preceding figure and you'll see that the artifact is extracted from hiberfil.sys. You can also see the addresses, which are very important for documentation.

How it works...

Magnet AXIOM walks through the hiberfil.sys (or pagefile.sys) file and extracts available webmail artifacts, such as Google’s Gmail, Microsoft’s Hotmail/Outlook.com, and Yahoo Mail.

See also

Modern windows hibernation file analysis:

`https://www.504ensics.com/uploads/publications/modern-windows-hibernation.pdf`

Skype forensics with Belkasoft Evidence Center

On modern Windows systems Skype is installed by default, so it's very important for a forensic examiner to extract user data from this application. This can be calls, messages, transferred or received files, and so on. In this recipe, we will show you how to parse these valuable artifacts with Belkasoft Evidence Center.

Getting ready

First of all, you should get a Skype profile folder. Again, you can use a forensic image, but to save time for testing purposes, we recommend using a profile folder as the data source. You can find Skype profile folders (yes, there can be more than one folder, as multiple accounts can be used on the same device) here:

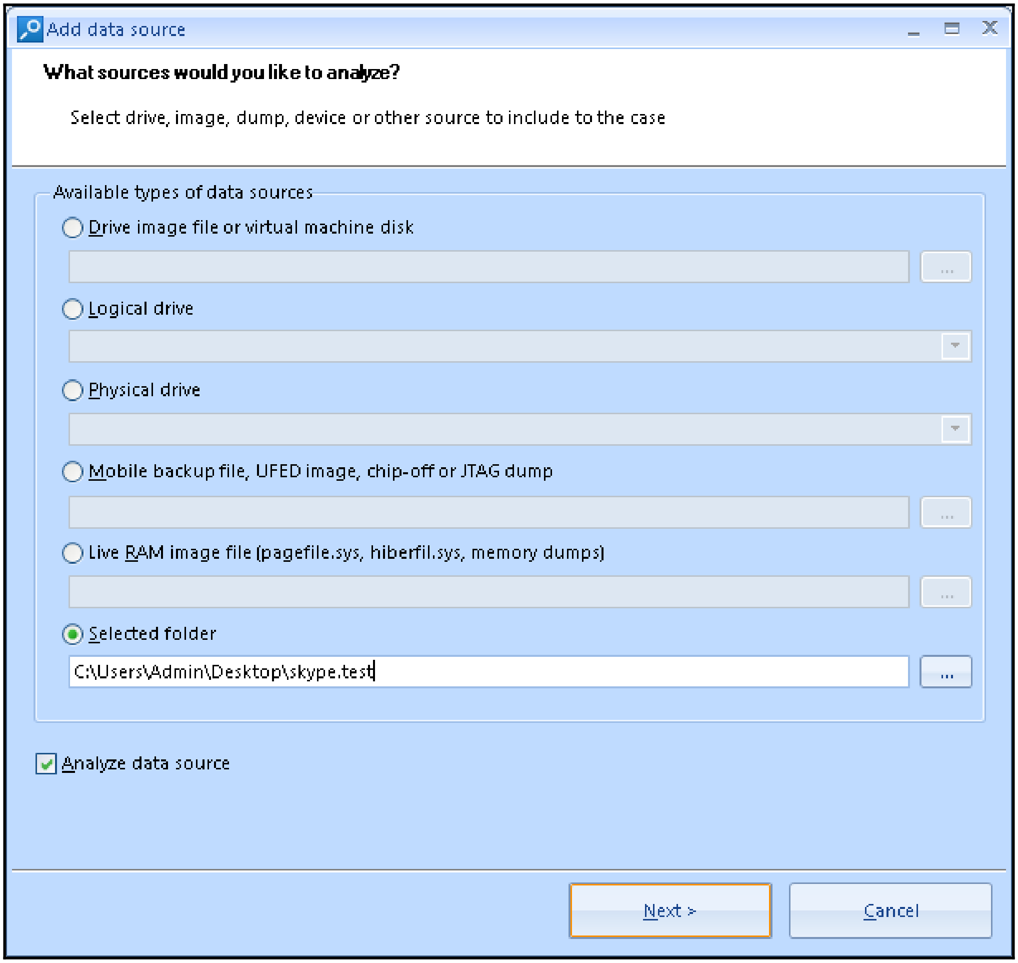
```
C:\Users\%USERNAME%\AppData\Roaming\Skype\
```

Once you get it, make sure Belkasoft Evidence Center (valid licence or trial) is installed on your workstation, and we are ready to start.

How to do it...

We can start the process by following the given steps:

1. Create a new case and add the profile folder you previously exported as the data source. Use **Selected folder**, as shown in the following figure:



Add data source

What sources would you like to analyze?

Select drive, image, dump, device or other source to include to the case

Available types of data sources

○ Drive image file or virtual machine disk

○ Logical drive

○ Physical drive

○ Mobile backup file, UFED image, chip-off or JTAG dump

○ Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)

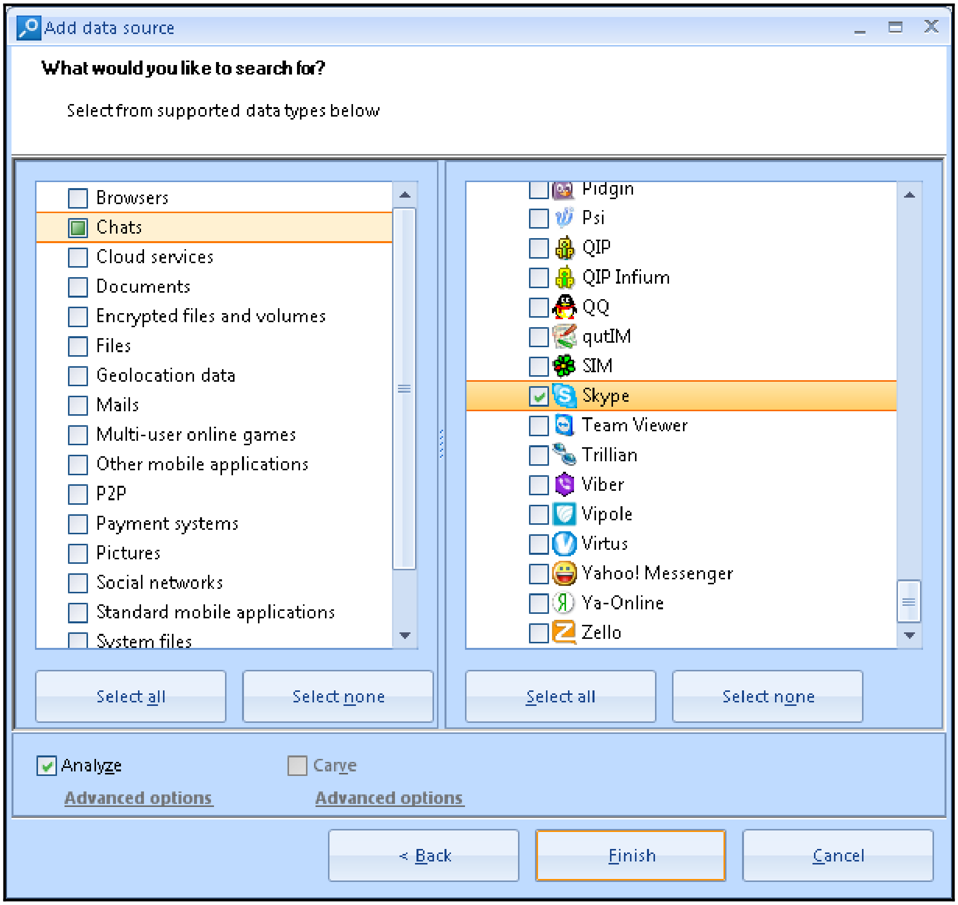
● Selected folder

C:\Users\Admin\Desktop\skype.test

☑ Analyze data source

Figure 9.17. Adding the data source in Belkasoft Evidence Center

2. Let's choose the right data type. We have a Skype profile folder, so go to **Chats**, find **Skype,** and tick it. Click **Finish** and wait a bit for the data to be parsed, as shown in the following screenshot:



Add data source

What would you like to search for?

Select from supported data types below

- □ Browsers
- ■ Chats
- □ Cloud services
- □ Documents
- □ Encrypted files and volumes
- □ Files
- □ Geolocation data
- □ Mails
- □ Multi-user online games
- □ Other mobile applications
- □ P2P
- □ Payment systems
- □ Pictures
- □ Social networks
- □ Standard mobile applications
- □ System files

- □ Pidgin
- □ Psi
- □ QIP
- □ QIP Infium
- □ QQ
- □ qutIM
- □ SIM
- ☑ Skype
- □ Team Viewer
- □ Trillian
- □ Viber
- □ Vipole
- □ Virtus
- □ Yahoo! Messenger
- □ Ya-Online
- □ Zello

☑ Analyze   □ Carve

Figure 9.18. Choosing data types in Belkasoft Evidence Center

3. Once the data is processed, you can work with the **Overview** or **Case Explorer** tabs to analyze the extracted data, including calls, messages (including voice), pictures, and so on. It's important to note that Belkasoft Evidence Center also extracts deleted messages from the Skype database (main.db), and analyzes `chatsync` files, which may include messages, that are not included in the main database.

How it works...

Belkasoft Evidence Center processes the data source specified by a computer forensic examiner, and extracts Skype artifacts from the available sources, including SQLite free lists, unallocated space, `chatsync` files, `pagefile.sys`, `hiberfil.sys`, and so on.

See also

Belkasoft Evidence Center Trial:

`https://belkasoft.com/trial`

Recovering Destroyed SQLite Evidence, iPhone/Android Messages, Cleared Skype Logs:

`https://belkasoft.com/recover-destroyed-sqlite-evidence-skype-and-iphone-logs`

Skype forensics with SkypeLogView

It's always good to have some free pieces of software in your toolkit. There are some free and open source tools for Skype forensics, and one of them is SkypeLogView by NirSoft. You are already familiar with some NirSoft tools, and in this recipe we will show you how to use SkypeLogView for Skype forensicating.

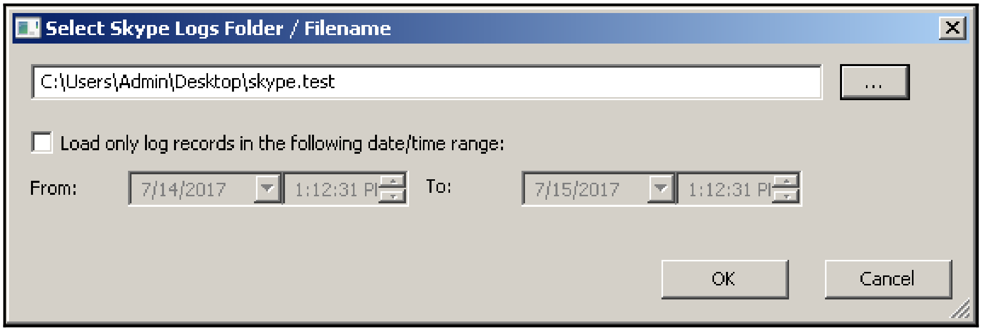
Getting ready

Download SkypeLogView from NirSoft's website (check the *See also* section for the download link). At the time of writing, the most recent version of the tool is 1.55. Unpack the archive and you are ready to go. You can use the Skype profile folder exported for the previous recipe.

How to do it...

We can start the process by following the given steps:

1. Start the tool, and you will see a data source window, like the one in the following figure:



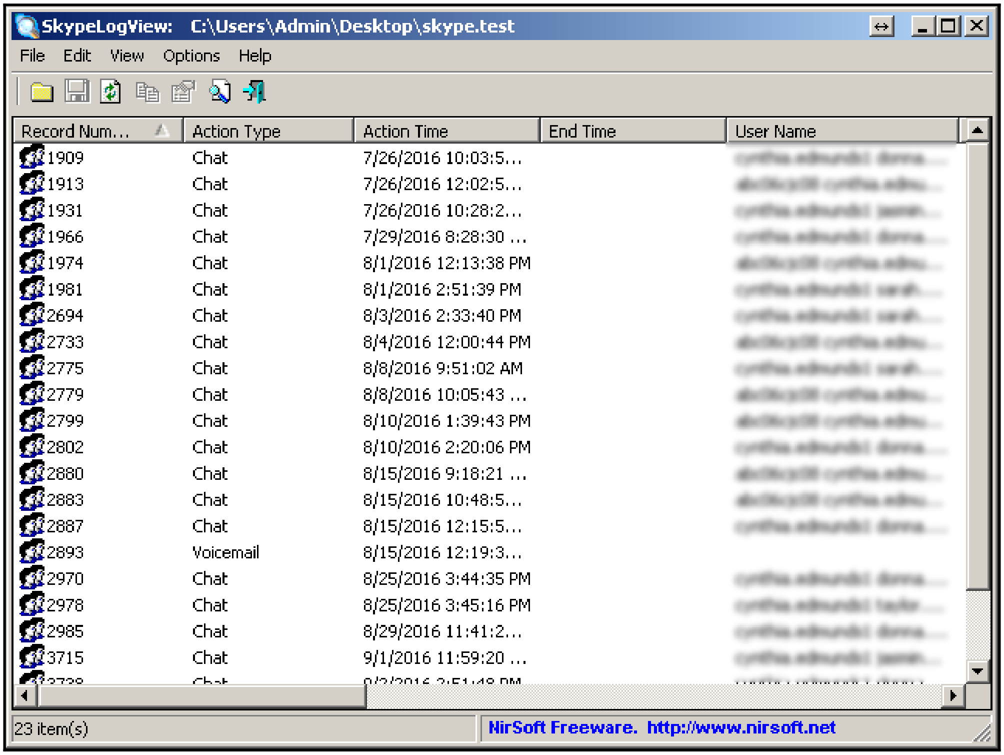
C:\Users\Admin\Desktop\skype.test

□ Load only log records in the following date/time range:

From: 7/14/2017 1:12:31 PM To: 7/15/2017 1:12:31 PM

Figure 9.19. Adding the data source in SkypeLogView

2. All you need now is to click **OK** and the magic begins, as shown in the following figure:



Record Num...	Action Type	Action Time	End Time	User Name
1909	Chat	7/26/2016 10:03:5...		[redacted]
1913	Chat	7/26/2016 12:02:5...		[redacted]
1931	Chat	7/26/2016 10:28:2...		[redacted]
1966	Chat	7/29/2016 8:28:30 ...		[redacted]
1974	Chat	8/1/2016 12:13:38 PM		[redacted]
1981	Chat	8/1/2016 2:51:39 PM		[redacted]
2694	Chat	8/3/2016 2:33:40 PM		[redacted]
2733	Chat	8/4/2016 12:00:44 PM		[redacted]
2775	Chat	8/8/2016 9:51:02 AM		[redacted]
2779	Chat	8/8/2016 10:05:43 ...		[redacted]
2799	Chat	8/10/2016 1:39:43 PM		[redacted]
2802	Chat	8/10/2016 2:20:06 PM		[redacted]
2880	Chat	8/15/2016 9:18:21 ...		[redacted]
2883	Chat	8/15/2016 10:48:5...		[redacted]
2887	Chat	8/15/2016 12:15:5...		[redacted]
2893	Voicemail	8/15/2016 12:19:3...		
2970	Chat	8/25/2016 3:44:35 PM		[redacted]
2978	Chat	8/25/2016 3:45:16 PM		[redacted]
2985	Chat	8/29/2016 11:41:2...		[redacted]
3715	Chat	9/1/2016 11:59:20 ...		[redacted]
3738	Chat	9/2/2016 2:51:48 PM		[redacted]

23 item(s)

NirSoft Freeware. http://www.nirsoft.net

3. Of course, you can sort the extracted data using different columns. If you want the timestamp to be displayed in GMT, go to **Options - Show Time in GMT**.
4. Finally, you can create an HTML report. To do this, go to **View - HTML Report**.

How it works...

SkypeLogView uses an examiner specified folder and extracts available Skype artifacts, such as chats, voicemails, calls, and so on. Also an examiner can create an HTML report for all or for user-selected artifacts.

See also

SkypeLogView download page:

`http://www.nirsoft.net/utils/skype_log_view.html`

10
Windows 10 Forensics

In this chapter, we will cover the following recipes:

- Parsing Windows 10 Notifications
- Cortana forensics
- OneDrive forensics
- Dropbox forensics
- Windows 10 mail app
- Windows 10 Xbox app

Introduction

The advent of Windows 10 has caused controversy among users and forensic investigators alike. Many end users have concerns regarding privacy and security, since the privacy settings that are automatically set up on devices with Windows 10 are not at all strong. Others have expressed concerns about the way Windows machines are now forcing users to migrate to Windows 10, even if they are happy with their current versions.

From a forensic perspective, Windows 10 presents a number of new and unique challenges. Most of the programs have been modified to look and feel more like the applications you would see on a smartphone or tablet, and a lot of them behave quite differently from their predecessors. The advent of Cortana has given forensic investigators even more data to work with, and the amount of data has also increased in line with the interconnected nature of many of the applications.

In this chapter, we will look at a few of the common features of Windows 10, and how forensic analysts can work with it.

Parsing Windows 10 Notifications

Windows 10 features notifications, called *Toast* notifications, which pop up in the bottom right of the screen. These can be set up for a number of different requirements, but are on by default for news relating to application updates and security.

It is possible for users to set up notifications to remind themselves of tasks, as well as events and email alerts. In this chapter, we will look at the usefulness of Windows 10 notifications in forensic investigations, and how to parse them.

Getting ready

Details of notifications are stored in the following location:

```
\Users\Username\AppData\Local\Microsoft\Windows\Notifications
```

The name of the database will differ depending on the build version of Windows 10 installed on the machine. From Anniversary onwards, they are stored in `wpndatabase.db`; before that, they can be found in `appdb.dat`.

How to do it...

The steps to be followed for parsing Windows 10 notifications are as follows:

1. Download a SQLite manager if you do not have one.
2. Open your SQLite manager and click **Open Database**.

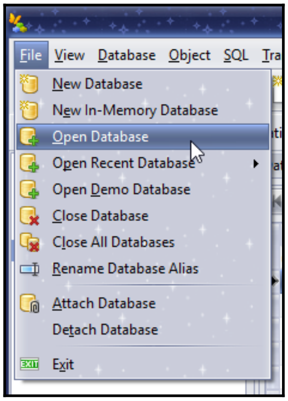
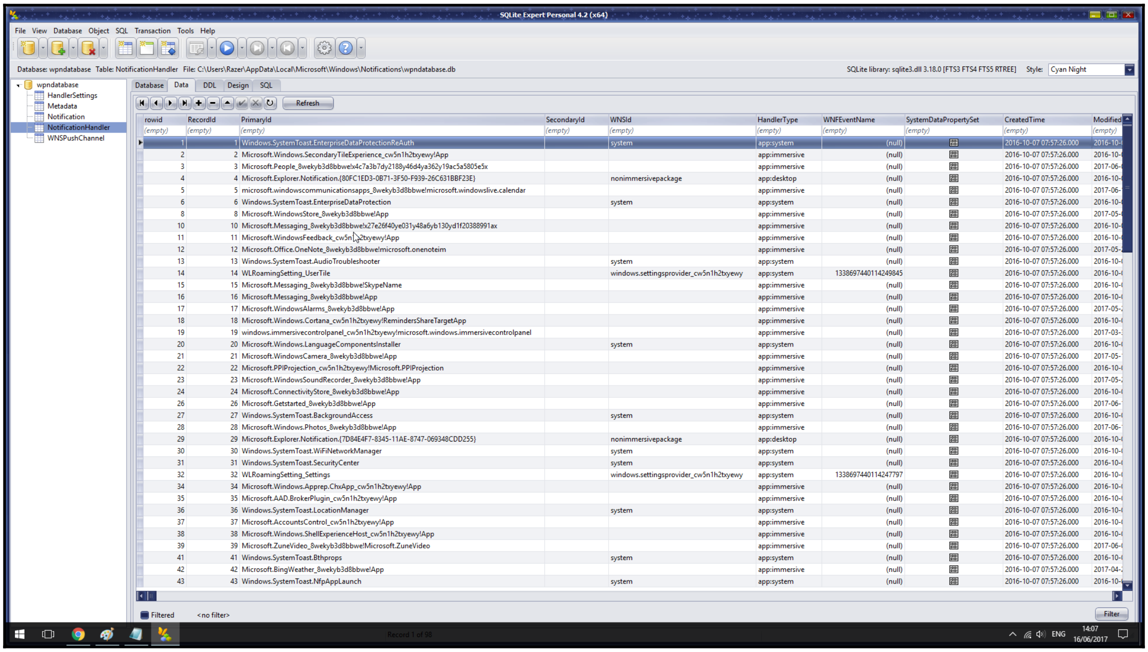


Figure 10.1. Adding a database

3. Browse to `C:\Users\Username\AppData\Local\Microsoft\Windows\Notifications` and find the `.db` file in the folder. Open it.



Database: wpndatabase Table: NotificationHandler File: C:\Users\Razer\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db

SQLite library: sqlite3.dll 3.18.0 [FTS3 FTS4 FTS5 RTREE] Style: Cyan Night

rowid	RecordId	PrimaryId	SecondaryId	WNSId	HandlerType	WNFEventName	SystemDataPropertySet	CreatedTime	Modified
(empty)	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)
1	1	Windows.SystemToast.EnterpriseDataProtectionReAuth		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
2	2	Microsoft.Windows.SecondaryTileExperience_cw5n1h2txyewy!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
3	3	Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-06-
4	4	Microsoft.Explorer.Notification.{80FC1ED3-0B71-3F50-F939-26C631BBF23E}		nonimmersivepackage	app:desktop	(null)	▦	2016-10-07 07:57:26.000	2016-10-
5	5	microsoft.windowscommunicationsapps_8wekyb3d8bbwe!microsoft.windowslive.calendar			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-06-
6	6	Windows.SystemToast.EnterpriseDataProtection		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
8	8	Microsoft.WindowsStore_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-05-
10	10	Microsoft.Messaging_8wekyb3d8bbwe!x27e26f40ye031y48a6yb130yd1f20388991ax			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
11	11	Microsoft.WindowsFeedback_cw5n1h2txyewy!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
12	12	Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-05-
13	13	Windows.SystemToast.AudioTroubleshooter		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
14	14	WLRoamingSetting_UserTile		windows.settingsprovider_cw5n1h2txyewy	app:system	1338697440114249845	▦	2016-10-07 07:57:26.000	2016-10-
15	15	Microsoft.Messaging_8wekyb3d8bbwe!SkypeName			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
16	16	Microsoft.Messaging_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
17	17	Microsoft.WindowsAlarms_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-05-
18	18	Microsoft.Windows.Cortana_cw5n1h2txyewy!RemindersShareTargetApp			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
19	19	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-03-
20	20	Microsoft.Windows.LanguageComponentsInstaller		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
21	21	Microsoft.WindowsCamera_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-05-
22	22	Microsoft.PPIProjection_cw5n1h2txyewy!Microsoft.PPIProjection			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
23	23	Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-05-
24	24	Microsoft.ConnectivityStore_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
26	26	Microsoft.Getstarted_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-06-
27	27	Windows.SystemToast.BackgroundAccess		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
28	28	Microsoft.Windows.Photos_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-06-
29	29	Microsoft.Explorer.Notification.{7D84E4F7-8345-11AE-8747-069348CDD255}		nonimmersivepackage	app:desktop	(null)	▦	2016-10-07 07:57:26.000	2016-10-
30	30	Windows.SystemToast.WiFiNetworkManager		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
31	31	Windows.SystemToast.SecurityCenter		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
32	32	WLRoamingSetting_Settings		windows.settingsprovider_cw5n1h2txyewy	app:system	1338697440114247797	▦	2016-10-07 07:57:26.000	2016-10-
34	34	Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
35	35	Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
36	36	Windows.SystemToast.LocationManager		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
37	37	Microsoft.AccountsControl_cw5n1h2txyewy!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
38	38	Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2016-10-
39	39	Microsoft.ZuneVideo_8wekyb3d8bbwe!Microsoft.ZuneVideo			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-06-
41	41	Windows.SystemToast.Bthprops		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-
42	42	Microsoft.BingWeather_8wekyb3d8bbwe!App			app:immersive	(null)	▦	2016-10-07 07:57:26.000	2017-04-
43	43	Windows.SystemToast.NfpAppLaunch		system	app:system	(null)	▦	2016-10-07 07:57:26.000	2016-10-

Filtered <no filter>

Record 1 of 98

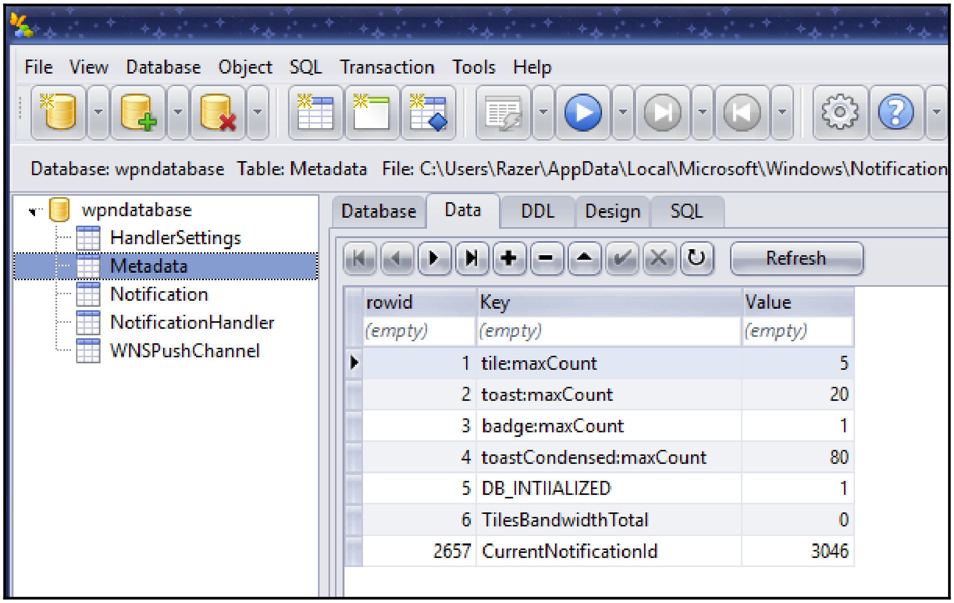
Figure 10.2. The notifications database file

This will show you which notifications have popped up, along with their RecordIDs, which can be used to identify other instances of these programs.

How it works...

A SQLite viewer will show you which programs have notifications popping up on a regular basis, and which have been disabled.

- In the example below, the user has seen 20 Toast notifications - the small rectangular boxes that pop up in the bottom right of the screen. However, there have only been five title notifications. This refers to an application's icon as seen on the Start menu. If the number of tile notifications is very low, this probably means that the user has unpinned a number of programs from the Start menu.



File View Database Object SQL Transaction Tools Help
Database: wpndatabase Table: Metadata File: C:\Users\Razer\AppData\Local\Microsoft\Windows\Notification
wpndatabase
HandlerSettings
Metadata
Notification
NotificationHandler
WNSPushChannel
Database Data DDL Design SQL
Refresh

rowid	Key	Value
(empty)	(empty)	(empty)
1	tile:maxCount	5
2	toast:maxCount	20
3	badge:maxCount	1
4	toastCondensed:maxCount	80
5	DB_INTIIALIZED	1
6	TilesBandwidthTotal	0
2657	CurrentNotificationId	3046

Figure 10.3. Notifications a user has seen

- The preceding image shows that the user has only seen one *Badge* notification. These are small numbers that pop up on the taskbar alongside a program - a bit like the little numerical values you see next to the notifications icons on Facebook or Twitter.

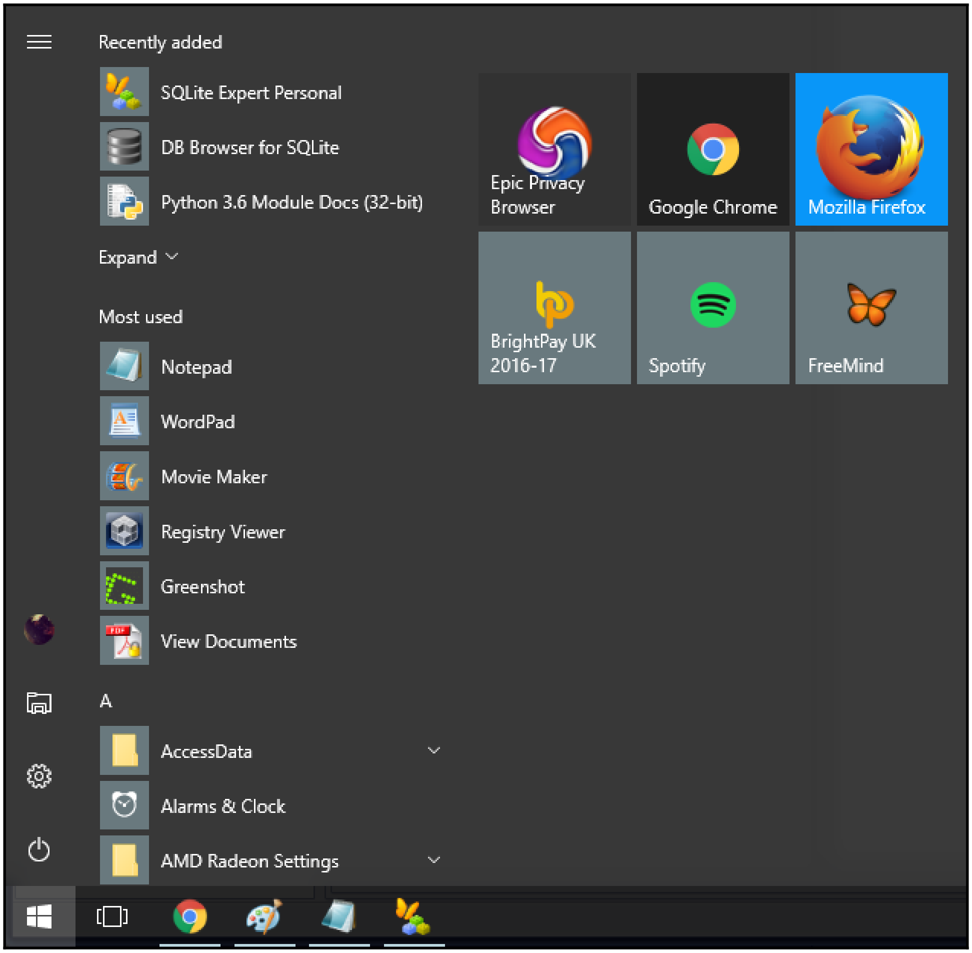


Figure 10.4. Tiles on the Start menu

- If you have turned off icons on the taskbar, you may see these notifications when you click on the up arrow next to the Wi-Fi and volume signs.

See also

- SQLite Expert download: `http://www.sqliteexpert.com/download.html`
- DB Browser for SQLite: `http://sqlitebrowser.org/`

Cortana forensics

Cortana is Microsoft's voice-activated assistant, but it does much more than just respond to commands. Cortana links in across different devices, giving reminders when required and *getting to know* the user. It can recognize an individual's voice and handwriting, among other things. For this reason, many Windows users have turned the Cortana function off due to privacy concerns - particularly because, by default on some machines, Cortana is always on, even when the machine is in sleep mode.

Cortana can also respond to specific occurrences - for example, a user can instruct Cortana to remind them to say something to a person next time they call. This is undoubtedly a useful tool for many, and also a mine of forensic information.

Getting ready

Forensically speaking, the most interesting tidbits of information when it comes to Cortana can be found in the following location:
`C:\Users[User]\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\LocalState\ESEDatabase_CortanaCoreInstance\CortanaCoreDb.dat`

Here you will be able to uncover information such as the locations the user has been in, the reminders they have set, where and when those reminders were triggered, and where and when the reminders were marked as complete.

This can be of particular interest if your case hinges on putting someone in a certain place at a certain time. Likewise, a reminder that has not been marked as complete may demonstrate that the user's plans changed at the last minute.

How to do it...

You will need a SQLite browser to access the database.

1. Once you have started up your SQLite browser and accessed the database, you will be able to see a table of values which will include useful items such as Contact Permissions and Locations.
2. You can work with this database directly in your SQLite browser, or you can export it to a CSV document which can then be opened with Microsoft Excel, Google Sheets or another program of your choice.

3. It is worth noting that some of the data in the `CortanaCoreDb.dat` file may be obscured. Depending on what you are looking for, once you have opened the file to ensure it contains some data, you may wish to run it through a more sophisticated forensic program to uncover the data.
4. The `Reminders` section of `CortanaCoreDb.dat` is concerned with calendar reminders, which can be a useful way to demonstrate a user's intentions. For example, they may have set a reminder to tell them to go to a given location at a set time, which may place them near a crime scene. If this is then teamed up with actual location data from the `CortanaCoreDb.dat` `LocationTriggers` section, it can be either damning or absolving evidence.

It is a good idea to go thoroughly through all the items in the `Cortana` folder at the path mentioned above. The most relevant data is likely to be contained in `CortanaCoreDb.dat`, however there are certain items - such as geolocation searches and some dictation records - that may be found in other parts of the folder. As always with forensic examination, it is worth digging through the evidence with a fine-toothed comb, at least insofar as time allows.

How it works...

Cortana works by essentially *listening* to, and being aware of, everything that is going on around a computer at a given time. This is even the case when the computer is locked, which is particularly of interest in forensic investigations. Often a computer user - especially with a laptop - will leave their computer on but with the screen sleeping for long periods of time, essentially forgetting that it is still turned on.

While this has caused understandable consternation among privacy advocates and members of the general public, it can be hugely useful for investigative purposes. Snippets of conversations, data about the location of the user, voice searches, reminders, and which device a person is using can all be uncovered through the methods detailed previously and can provide priceless clues to a person's actions and motivations.

See also

Bhupendra Singh; *A Forensic insight into Windows 10 Cortana Search*; *Computers & Security Vol. 66*, May 2017

Thomas Rose; *A Forensic Investigation of the Windows Search Feature, Cortana and the Notification Centre in Windows 8/8.1 and Windows 10*; BSc dissertation 2016

OneDrive forensics

OneDrive is Microsoft's cloud service, which allows users to save their data on the cloud and access it from any machine, as long as they are logged in with their Microsoft account. Featuring Word, Excel, PowerPoint, Outlook, a calendar, contacts, and more, this is a straightforward way for users of Microsoft products to ensure that they never lose access to their documents. It is also a great source of information and data in forensic investigations.

One way in which OneDrive is especially useful to forensic investigators is in instances where a particular device cannot be accessed for one reason or another. For example, perhaps a phone has been seized, but it is locked and the passcode cannot be retrieved; or perhaps a computer has a password that has proven too difficult to bypass. In these instances, if the investigator can gain access to a different device owned by the same user, they can often find useful tidbits of information in the OneDrive backup files.

In the Windows 10 operating system, OneDrive is the default location to save new files, rather than these being saved in My Documents on the local computer, which was previously the default. This means that, unless the user has manually changed their settings, there should be a wealth of forensic information available via OneDrive.

Getting ready

First of all, it is important to work out how you are going to access your OneDrive files. Do you have access to the Windows 10 machine itself, or are you looking at an Android backup?

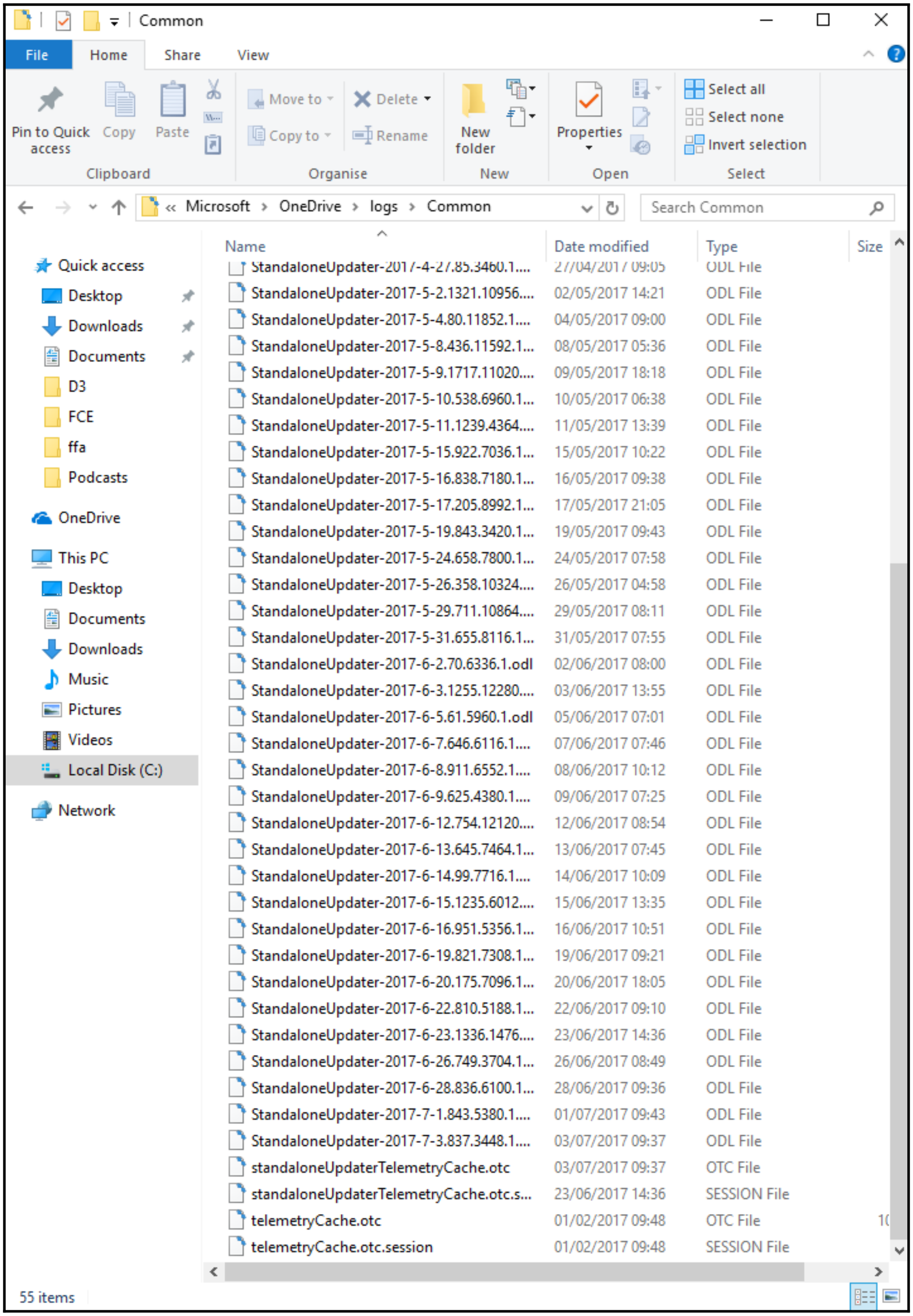
If you are accessing OneDrive using an Android phone, you will find what you need in `/mnt/sdcard/Android/data/` under the `com.microsoft.skydrive` folder. OneDrive's predecessor was called SkyDrive, hence the name.

If you are accessing OneDrive data using a PC or a laptop running Windows 10, you will find what you need in `C:\Users\<USERNAME>\AppData\Local\Microsoft\OneDrive\logs`.

How to do it...

The following steps need to be followed to perform forensics on OneDrive:

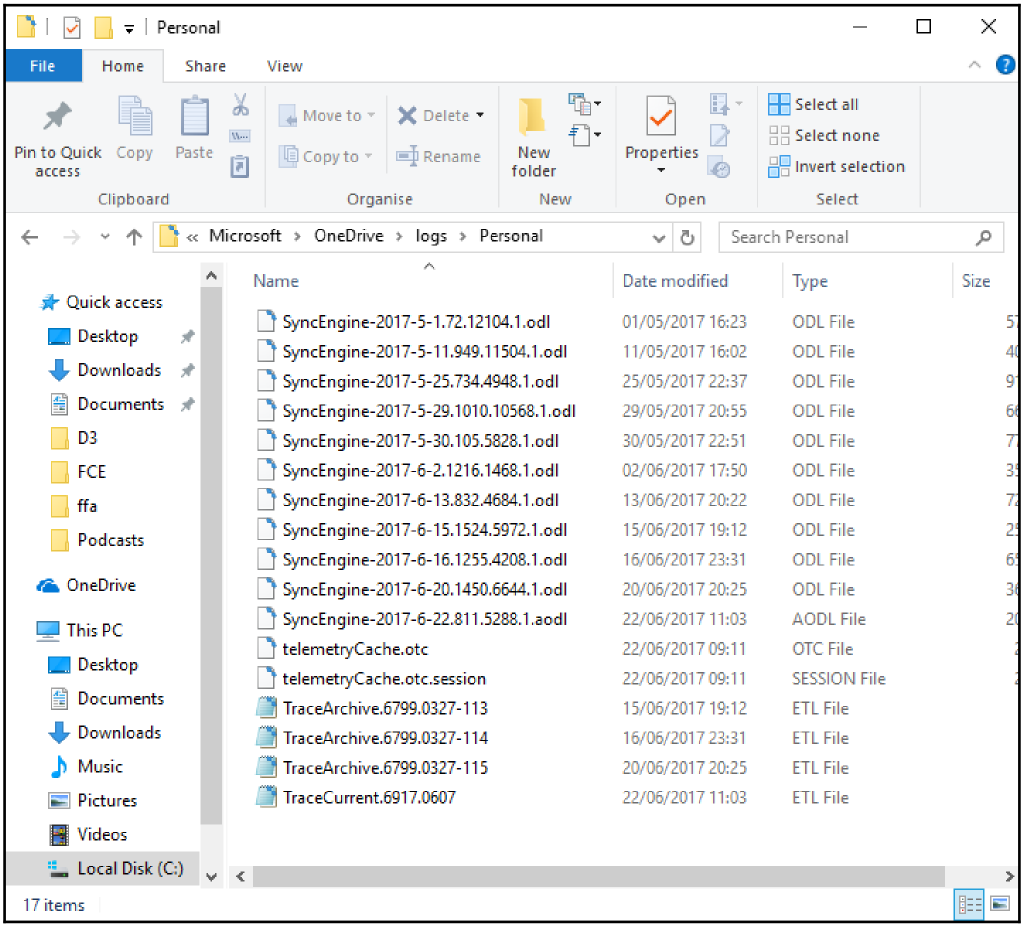
1. Open your forensic software of choice and navigate to the relevant folder, depending on whether you are using a smartphone or a computer for forensic analysis (see the previous paragraphs for details).
2. The backend of the OneDrive folder is actually not of particular forensic interest. In the `logs` folder listed above you will find two subfolders: `Common` and `Personal`. The `Common` folder lists all elements the operating system automatically runs, namely `StandaloneUpdater` and `telemetryCache` files. These refer to automated updates to OneDrive.



Name	Date modified	Type	Size
StandaloneUpdater-2017-4-27.85.3460.1....	27/04/2017 09:05	ODL File	
StandaloneUpdater-2017-5-2.1321.10956....	02/05/2017 14:21	ODL File	
StandaloneUpdater-2017-5-4.80.11852.1....	04/05/2017 09:00	ODL File	
StandaloneUpdater-2017-5-8.436.11592.1....	08/05/2017 05:36	ODL File	
StandaloneUpdater-2017-5-9.1717.11020....	09/05/2017 18:18	ODL File	
StandaloneUpdater-2017-5-10.538.6960.1....	10/05/2017 06:38	ODL File	
StandaloneUpdater-2017-5-11.1239.4364....	11/05/2017 13:39	ODL File	
StandaloneUpdater-2017-5-15.922.7036.1....	15/05/2017 10:22	ODL File	
StandaloneUpdater-2017-5-16.838.7180.1....	16/05/2017 09:38	ODL File	
StandaloneUpdater-2017-5-17.205.8992.1....	17/05/2017 21:05	ODL File	
StandaloneUpdater-2017-5-19.843.3420.1....	19/05/2017 09:43	ODL File	
StandaloneUpdater-2017-5-24.658.7800.1....	24/05/2017 07:58	ODL File	
StandaloneUpdater-2017-5-26.358.10324....	26/05/2017 04:58	ODL File	
StandaloneUpdater-2017-5-29.711.10864....	29/05/2017 08:11	ODL File	
StandaloneUpdater-2017-5-31.655.8116.1....	31/05/2017 07:55	ODL File	
StandaloneUpdater-2017-6-2.70.6336.1.odl	02/06/2017 08:00	ODL File	
StandaloneUpdater-2017-6-3.1255.12280....	03/06/2017 13:55	ODL File	
StandaloneUpdater-2017-6-5.61.5960.1.odl	05/06/2017 07:01	ODL File	
StandaloneUpdater-2017-6-7.646.6116.1....	07/06/2017 07:46	ODL File	
StandaloneUpdater-2017-6-8.911.6552.1....	08/06/2017 10:12	ODL File	
StandaloneUpdater-2017-6-9.625.4380.1....	09/06/2017 07:25	ODL File	
StandaloneUpdater-2017-6-12.754.12120....	12/06/2017 08:54	ODL File	
StandaloneUpdater-2017-6-13.645.7464.1....	13/06/2017 07:45	ODL File	
StandaloneUpdater-2017-6-14.99.7716.1....	14/06/2017 10:09	ODL File	
StandaloneUpdater-2017-6-15.1235.6012....	15/06/2017 13:35	ODL File	
StandaloneUpdater-2017-6-16.951.5356.1....	16/06/2017 10:51	ODL File	
StandaloneUpdater-2017-6-19.821.7308.1....	19/06/2017 09:21	ODL File	
StandaloneUpdater-2017-6-20.175.7096.1....	20/06/2017 18:05	ODL File	
StandaloneUpdater-2017-6-22.810.5188.1....	22/06/2017 09:10	ODL File	
StandaloneUpdater-2017-6-23.1336.1476....	23/06/2017 14:36	ODL File	
StandaloneUpdater-2017-6-26.749.3704.1....	26/06/2017 08:49	ODL File	
StandaloneUpdater-2017-6-28.836.6100.1....	28/06/2017 09:36	ODL File	
StandaloneUpdater-2017-7-1.843.5380.1....	01/07/2017 09:43	ODL File	
StandaloneUpdater-2017-7-3.837.3448.1....	03/07/2017 09:37	ODL File	
standaloneUpdaterTelemetryCache.otc	03/07/2017 09:37	OTC File	
standaloneUpdaterTelemetryCache.otc.s...	23/06/2017 14:36	SESSION File	
telemetryCache.otc	01/02/2017 09:48	OTC File	1(
telemetryCache.otc.session	01/02/2017 09:48	SESSION File	

Fig 10.5 StandaloneUpdater and telemetryCache files in the Common folder

3. The `Personal` folder contains `SyncEngine`, `telemetryCache` and `TraceArchive` files. These files are updated automatically every few days. Generally, what can be found in them is not of great forensic interest; they are simply automated backups of the user's computer, but the files themselves do not contain any information. The only potential forensic application would be to demonstrate lack of use: for example, a frequent computer user who had disappeared and not turned on any of their Windows machines would show an unusual lack of activity in the OneDrive log files. The files are as shown in the following screenshot:



Name	Date modified	Type	Size
SyncEngine-2017-5-1.72.12104.1.odl	01/05/2017 16:23	ODL File	57
SyncEngine-2017-5-11.949.11504.1.odl	11/05/2017 16:02	ODL File	40
SyncEngine-2017-5-25.734.4948.1.odl	25/05/2017 22:37	ODL File	9
SyncEngine-2017-5-29.1010.10568.1.odl	29/05/2017 20:55	ODL File	66
SyncEngine-2017-5-30.105.5828.1.odl	30/05/2017 22:51	ODL File	77
SyncEngine-2017-6-2.1216.1468.1.odl	02/06/2017 17:50	ODL File	35
SyncEngine-2017-6-13.832.4684.1.odl	13/06/2017 20:22	ODL File	72
SyncEngine-2017-6-15.1524.5972.1.odl	15/06/2017 19:12	ODL File	25
SyncEngine-2017-6-16.1255.4208.1.odl	16/06/2017 23:31	ODL File	65
SyncEngine-2017-6-20.1450.6644.1.odl	20/06/2017 20:25	ODL File	36
SyncEngine-2017-6-22.811.5288.1.aodl	22/06/2017 11:03	AODL File	20
telemetryCache.otc	22/06/2017 09:11	OTC File	2
telemetryCache.otc.session	22/06/2017 09:11	SESSION File	2
TraceArchive.6799.0327-113	15/06/2017 19:12	ETL File	
TraceArchive.6799.0327-114	16/06/2017 23:31	ETL File	
TraceArchive.6799.0327-115	20/06/2017 20:25	ETL File	
TraceCurrent.6917.0607	22/06/2017 11:03	ETL File	

Fig 10.6. Files found within the Personal folder

4. Of course, the frontend of OneDrive is quite another matter. This has a wealth of information available to forensic examiners if they are able to access it. OneDrive files themselves are generally not password-protected, so all you will need is the pass code for the device on which they are being accessed in order to proceed.
5. There is also a Windows OneDrive app on the iTunes app store, so if you know that the subject of your investigation uses a mixture of Windows and Apple machines, this is worth looking out for.

There are no restrictions to the types of files that can be uploaded to OneDrive. However, the most common ones are those in the Microsoft Office suite: Word documents, Excel spreadsheets, PowerPoint presentations and so on. OneDrive files are not stored on the local machine, but can be accessed there using the OneDrive app. They can also be accessed using a web browser, as long as the computer is connected to the internet. As well as computers and smartphones, OneDrive files can also be accessed from Xbox consoles.

Any forensic software that can open traditional Microsoft Office files will be able to extract OneDrive files for viewing. Once the information within the files has been compared with metadata such as the last accessed date and time, it is possible to construct a more thorough outline of the case.

How it works...

OneDrive works slightly differently depending on whether a user has a Personal or Business account, and it is important to understand these differences as they may have a bearing on your forensic investigation.

When OneDrive syncs a file from your computer to the cloud, there is a small modification that takes place in OneDrive for Business. This version of OneDrive automatically adds a few lines of code to the beginning of documents when they are uploaded. This has strong forensic implications as it means that the original MD5 hashes don’t match, and can also mean that the files themselves grow slightly larger in size. This appears to happen whenever such a file is opened, even if no modifications are made - it is part of the automated syncing process. So, if you are analyzing a OneDrive for Business file, make sure you account for this as part of your process, or you may end up with some sticky questions should the case go to court!

See also

Daryabar, Farid; Dehghantanha, Ali; Eterovic-Soric, Brett & Choo, Kim-Kwang Raymond; *Forensic Investigation of OneDrive, Box, GoogleDrive and Dropbox Applications on Android and iOS Devices; Australian Journal of Forensic Sciences*, 48:6, 615-642, DOI: 10.1080/00450618.2015.1110620

Dropbox forensics

In an apparent attempt to make user transition between smartphones, tablets, and PCs more fluid, in version 8 and up, Microsoft have renamed their programs *applications* and have given the desktop a more smartphone-like feel.

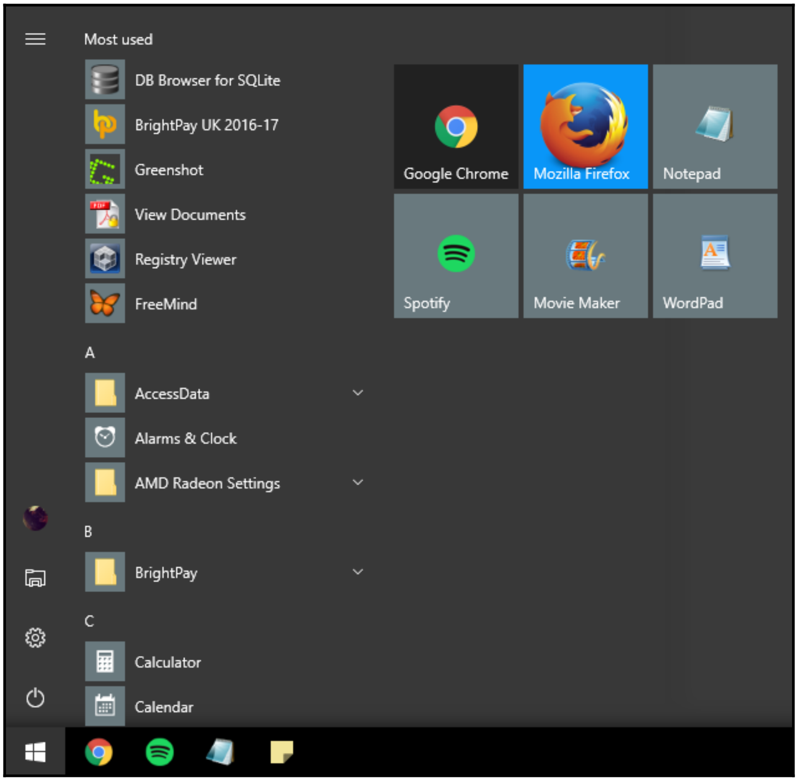


Fig 10.7. The Start menu now includes Tiles, which gives the computer more of a smartphone feel

Rather than downloading programs from a web browser, users can now shop for apps - many of which are free - that make for a smoother user experience.

Dropbox is a file sharing application that allows users to upload files of almost any type and easily share them with others. All that is required is an email address to sign up. In 2016, Dropbox had 500 million users worldwide, and this number is climbing.

Forensically, file sharing between users can provide a wealth of helpful information. Let's have a look at how to glean data from the Dropbox app.

Getting ready

Most of the Dropbox information you will require can be viewed with a simple SQLite browser, like the one we used in the section on Cortana forensics above.

However, some of the more interesting information may be encrypted, and to access that we will need a Dropbox decryptor. Magnet Forensics provide a free one which can be downloaded from their website, a link to which can be found at the end of the recipe.

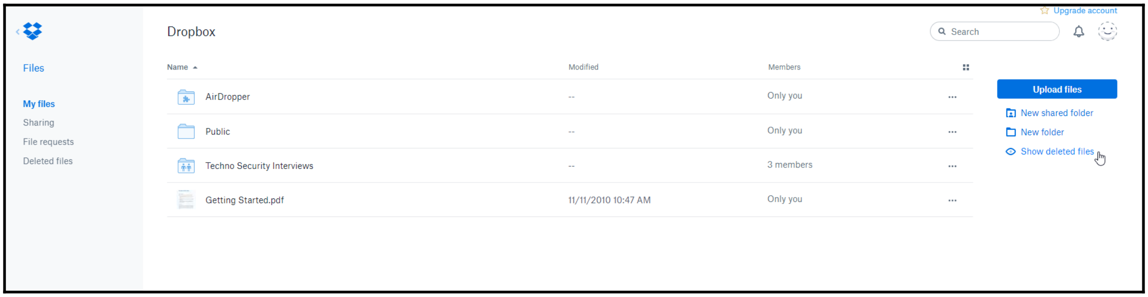
You will find all Dropbox-related information in `C:\Users\<USERNAME>\AppData\Local\Microsoft\Dropbox`.

How to do it...

The steps to be followed for dropbox forensics are as follows:

1. Open your SQLite browser and navigate to: `C:\Users\<USERNAME>\AppData\Local\Microsoft\Dropbox`. You will find several `.db` files contained within this folder.
2. The most interesting file in the folder is `filecache.db`. This lists all files and folders within the Dropbox account, as long as they have not been deleted. You can find details of how large each file is in `sigstore.db` in the same folder. The filecache database is encrypted by default, but this is one of those that can be decrypted by Magnet's Dropbox Decryptor, which will allow you to see not only the file names but also any associated metadata.

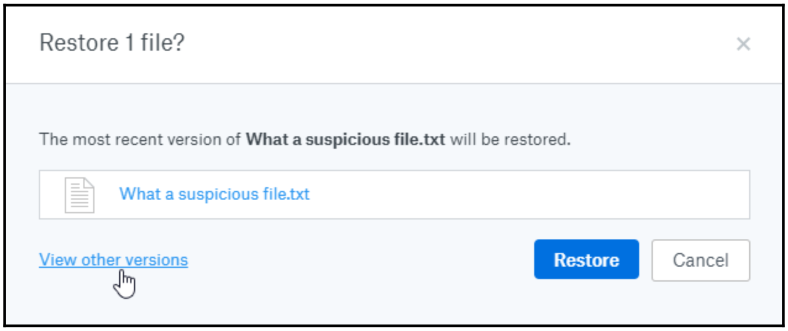
3. The Dropbox Decryptor will also uncover information from the `config.db` file, including the email address the account owner used to register, and a list of files that have recently been changed. This is particularly of interest in investigations where a person may be trying to cover their tracks. In some cases, Dropbox files will have been deleted. Deleted files are not kept on the local machine and so cannot be accessed strictly through Windows 10 forensic methods. However, if you know the username and password for the account, the web-based version of Dropbox does keep these files in the cloud. The amount of time for which they are kept depends on the type of account: for free accounts, deleted files are kept for 30 days; for premium (paid) accounts, they are kept forever.
4. Finding deleted files is easy on Dropbox. All you need to do is hover over the **Show deleted files** option on the right-hand side of the page.



Name	Modified	Members
AirDropper	--	Only you
Public	--	Only you
Techno Security Interviews	--	3 members
Getting Started.pdf	11/11/2010 10:47 AM	Only you

Fig 10.8. An option allows users to see deleted files

Once you can see the file that has been deleted, you can then click on **Restore** to view it. This will bring up a little box where it is worth clicking on the **View other versions** link under the main text as shown in the following screenshot:

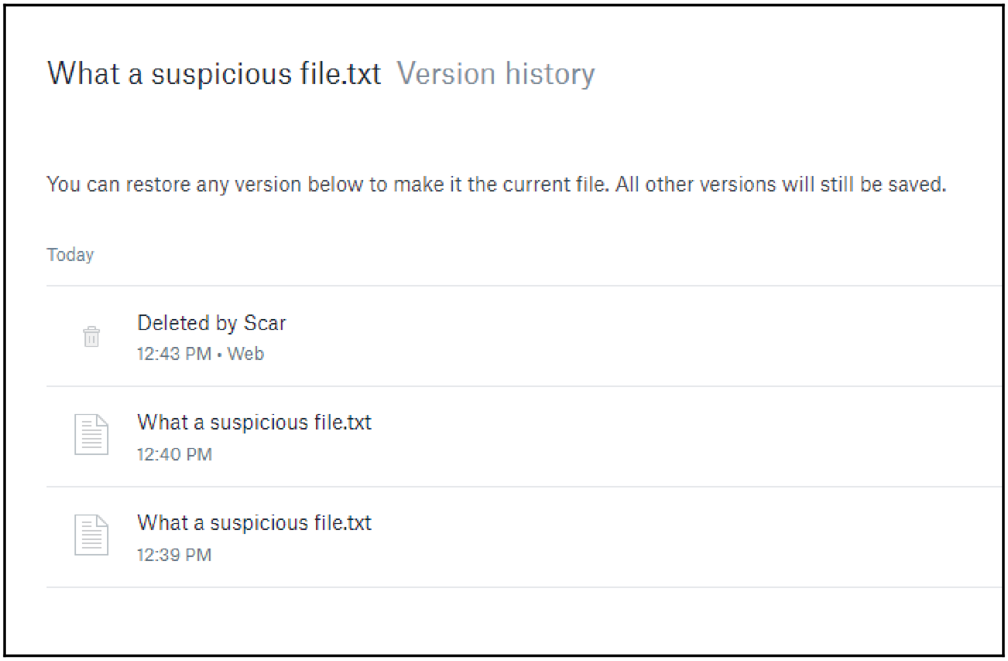

Restore 1 file?

The most recent version of **What a suspicious file.txt** will be restored.

What a suspicious file.txt

Fig 10.9. The 'View other versions' option can be forensically helpful

The following screenshot shows you how many versions of a file there have been, when they were edited, and when the file was deleted:



What a suspicious file.txt Version history

You can restore any version below to make it the current file. All other versions will still be saved.

Today

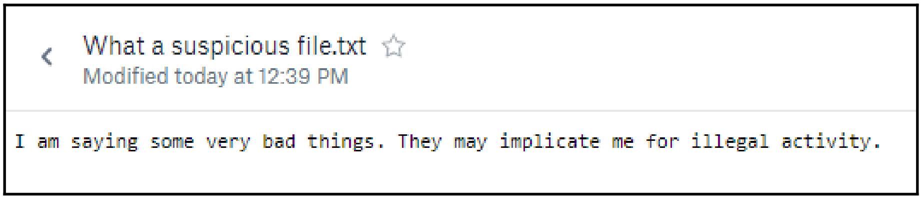
Deleted by Scar
12:43 PM • Web

What a suspicious file.txt
12:40 PM

What a suspicious file.txt
12:39 PM

Fig:10.10 . You will be able to see names and modification dates of file versions

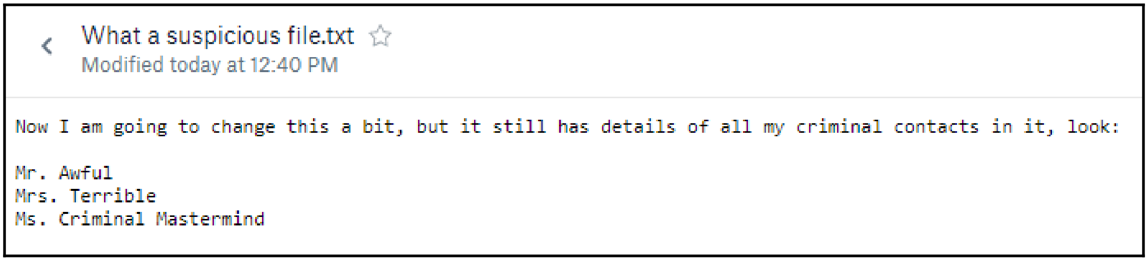
Clicking on each of these in turn will show you a preview version of the file itself, which can then be compared against other versions:



What a suspicious file.txt
Modified today at 12:39 PM

```
I am saying some very bad things. They may implicate me for illegal activity.
```

The two versions may be quite different even if they have the same file names, as you can see by comparing the figures:



```
Now I am going to change this a bit, but it still has details of all my criminal contacts in it, look:

Mr. Awful
Mrs. Terrible
Ms. Criminal Mastermind
```

It is then possible to see the contents of each file version

How it works...

Dropbox essentially works by backing up files on the cloud, although unlike certain other cloud-based applications, it only does so when a user manually adds a file, rather than automatically updating the contents of a machine. This can be useful for demonstrating intent.

Dropbox forensic techniques work by accessing either the databases left by the Dropbox application on the Windows machine, or by the investigator gaining access to the online Dropbox account and sifting through the files contained within.

See also

Magnet Forensics' Dropbox Decryptor: `https://www.magnetforensics.com/free-tool-dropbox-decryptor/` (accessed 05/07/17)

Windows 10 mail app

The Windows 10 Mail app is similar to previous apps in terms of user experience, however there is a number of forensic differences. The main one is the way in which emails are stored. They are no longer saved as `.eml` files; rather, they are now saved as HTML or `.txt` files.

Another neat feature in the new Mail app is the ability to connect to multiple accounts. Much like Gmail, Mail now comes with the ability to switch between different accounts - and users can now add other email providers such as Gmail and Yahoo to their Microsoft Mail apps.

Getting ready

Several forensic tools will be able to extract data from the Mail app. In this example, we are going to talk about FTK Imager, but the process of extracting data and especially elements such as file paths and folder locations, will be the same regardless of which tool you prefer to use.

First of all, open up FTK Imager and add a new evidence item. The data you are looking for will be in the `\Users\Username\AppData\Local\Comms` folder.

Opening this folder, you will see five subfolders: `Temp`, `Unistore`, `UnistoreDB`, `UserDataTempFiles`, and `Volatile`. These are the locations we will be looking at in this chapter.

How to do it...

The `data` folder contains a wealth of useful information, but it is sequestered away in subfolders:

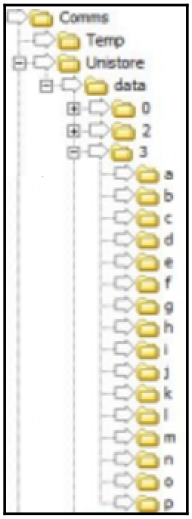


Fig 10.11 Some of the subfolders within the 'data' folder

1. The subfolders we are particularly interested in for the purposes of this chapter are 3 and 7, which refer respectively to mail and attachments. Within these subfolders are more subfolders, each one's name corresponding to a letter of the alphabet. It is inside these folders that the data we are looking for can be found.
2. Since the emails are now stored in HTML or plain text, it is easy to view their contents. Simply click on the `.dat` files within the alphabetically-named subfolders and you will be able to see a preview of the message within FTK. To view any attachments, navigate to folder `7` and go through its alphabetical subfolders. These messages and attachments can then be exported into a report for your client.

   Some emails are not sent, and bits of these may be found in the `UserDataTempFiles` folder in `\Users\Username\AppData\Local\Comms`. This data is volatile and frequently overwritten, so there may not be anything useful in there. However, on occasion you will find fragments of messages from which certain information may be extracted.

3. One final noteworthy element in the Mail app is the `People` folder. This contains all the contacts to whom a user has sent emails to in the past. You can access this data in `\Users\Username\AppData\Local\Comms\UniStoreDB\store.vol\Contact`

   The three most interesting elements here are the `Contacts.txt` and `Pcontacts.txt` files, which show the names and email addresses of the user's contacts. If they have stored extra information, such as a contact's address or telephone number, this will also be available in plain text within these files.

How it works...

The Mail app is native to the user's machine, although an increasing number of people are moving to Microsoft's cloud-based service instead, which as discussed in the previous section presents certain forensic challenges.

Basic information, such as contacts with whom the user frequently interacts, is stored in the `\Users\Username\AppData\Local\Comms` folder so that it can be easily recalled when the user wants to send a new message. Luckily, this also makes it available for forensic investigation!

Windows 10 Xbox App

As the name suggests, Windows 10's Xbox application allows users to play Xbox games on their Windows 10 machines. At first glance, this may not sound like a particularly forensically interesting source of information. However, looking under the hood we can find a wealth of data that can be leveraged in investigations. This section will take you through how to do that.

Getting ready

The information we are looking for can all be found in the `Packages` directory at the following location:

```
\Users\Username\AppData\Local\LocalState\ModelManager
```

You are looking for the `Xboxlivegamer.xml` file, which contains information that may be relevant to your case. Also, since Xbox is a gaming platform and many people use it only for leisure purposes, it is one location a user may have overlooked if they have taken anti-forensic measures.

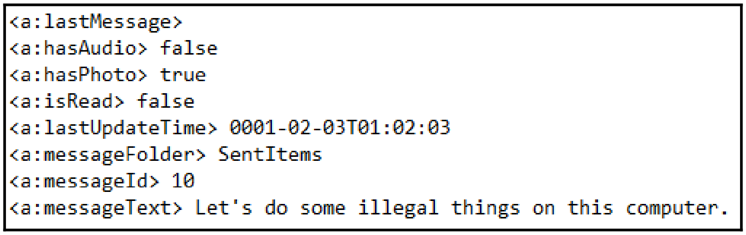
Since the vast majority of the files we will be looking at are `.xml` files, you do not need any extra forensic software to access the data. However, most well-known softwares, such as FTK, EnCase and so on, will be able to examine the files and their metadata.

How to do it...

The steps to be followed for Windows 10 Xbox app forensics are as follows:

1. Navigate to the location listed above and browse through the file list.
2. Within `Xboxlivegamer.xml` you will find the user's profile details, including their avatar and email address.
3. Going down one subfolder, into `\Users\Username\AppData\Local\LocalState\ModelManager\People`, will allow you to look at social connections.
4. To find details of contacts, including messaging, relationships, and information about their friends, you will need to look at the `.xml` file that is named after the user's Xbox ID. You can find this ID in the `Xboxlivegamer.xml` file.

5. Along with all the usual data on friends, you should also be able to see the listed locations of friends, which can be particularly interesting if you are trying to establish whether a person is linked in any way to a specific place.
6. A very useful place to look is in the `Messaging` subfolder, which contains details of all messages sent and received, including timestamps, the users who sent or received them, and the messages themselves in plain text:



```
<a:lastMessage>
<a:hasAudio> false
<a:hasPhoto> true
<a:isRead> false
<a:lastUpdateTime> 0001-02-03T01:02:03
<a:messageFolder> SentItems
<a:messageId> 10
<a:messageText> Let's do some illegal things on this computer.
```

Fig:10.11.Message data from the Xbox app

7. Recording gameplay is something a lot of users do, either to post it on the internet later or to refine techniques, or simply to share it with friends. However, some people also use this handy built-in feature of the Xbox app to record their screens when running various other applications. You can find the recorded gameplay data in `\Users\Username\XboxApp\GameDVR\OnThisPC`. Within this folder you should see a subfolder called `Videos`, which in turn contains a folder called `Captures`. You will then be able to open and play these videos.

How it works...

The Xbox app essentially brings the experience of an Xbox gaming environment to a Windows 10 PC. It stores data in plain text and as original video files, making it a repository of useful information in forensic examinations.

11
Data Visualization

In this chapter, we will cover the following recipes:

- Data visualisation with FTK
- Making a timeline in Autopsy
- Nuix's Web Review & Analytics

Introduction

Being able to accurately view and analyze results is an important part of any investigation. Even before the final results stage, however, it can be useful to be able to look at and manipulate different factors within a case, so as to work out where it might be necessary to drill down further, and to uncover correlations that otherwise may be overlooked.

While the primary goal of digital forensics tools is not to look pretty but to uncover, analyze, and report back on data, the visualization process is nonetheless an important part of any software.

A well put together data visualization tool can demonstrate links between contacts, build a timeline and identify potential points of interest along it, bring to light geographical areas that may be relevant to an investigation, and give basic statistical outputs that can lead an investigator to understand which steps should be taken next, among other things.

In this chapter, we will be looking at data visualization techniques and options in three forensic suites. First, we will look at **AccessData's** FTK and how it reports visually on important areas for investigation. We will then go through open-source freeware Autopsy and discuss how to create a timeline. Finally, we will take a look at Nuix's suite of forensic tools, including their new Web Review & Analytics add-on which sits on top of Nuix Investigator Lab.

Data visualization with FTK

This tool allows you to create and filter timelines, split data into categories, view emails and related metadata, analyze traffic and social connections, and observe geolocation data in a user-friendly environment. It also allows the user to specify a particular theme or color scheme, giving it a customizable feel.

Getting ready

Open FTK and load up a case (if you are not sure how to do this, see the section *Drive acquisition in E01 format with FTK Imager* in `Chapter 3`, *Windows Drive acquisition.)*

Choose a dataset within the case, then click the visualization icon in the top right-hand side of the screen. This will launch the visualization tool.

How to do it...

There are various possible uses for the visualization tool, so we will go through them one at a time:

1. Firstly, you can change the theme of FTK should you wish to do so. You can do this by going to **CaseManager|Tools|Preferences** in FTK, which will then open up a box which lists several options. These correspond closely to the options that used to be available in older versions of Windows, so it should be familiar to many.
2. One of the most useful items in the visualization toolset is the timeline feature, which allows a user to view actions on a device over a specific time period.
    1. First you must tell FTK which dates you want to focus on. You can do this by selecting a range of dates in the timeline section.
    2. Once your date range has been loaded in the Timeline, you will see three horizontal sections on the page:
        - The first section is the timeline itself, which shows different items of interest within the range of dates you have specified.

- The middle section is the Dashboard, which adds extra details about the data in the timeline. Here you can see your data broken down by category - for example, the percentage of emails compared with images, files, and other items of interest.
- Similarly, the bottom section is the Data List, which is structured similar to the rest of FTK and so should be easy to navigate. Like the name suggests, it provides a list of items that can then be selected individually should you wish to drill down further.

3. Once you have a date range in front of you, it is then possible to zoom in on a more specific time frame. For example, if you can see that a lot of activity has happened on a specific date, you can use the sliders to look only at that date in more detail. Likewise, you can focus on a specific hour, minute, or even second.
4. Taking a look at the Dashboard section in more detail, if you select the **Categories Distribution Chart** on the **Overview** tab, it will zoom in and show you your data broken down into categories. These will vary depending on your case, however popular options include folders, documents, emails, and graphics.
5. If you click on any particular category, it will then show up in the **Data List** pane at the bottom of the screen. This will allow you to sort and analyze data within a specific category. Sorting the data is easy: simply click on the heading that you are interested in and drag it onto the blue bar above. Once you have sorted your data, you can then scan the list and mark any items that should be explored further. To mark an item, select it in the **Data List** and then choose **Mark Selected Items** on the right-hand side of the screen. A box will then pop up which gives you various choices, including adding a label or creating a bookmark.

Let’s take the example of an email — say you have found a message of interest and want to learn more about who sent it and what their motivations might have been. The easiest way to do this is using the Social Analyzer tool. To access this, simply select the email you want to find out about and then click **Social Analyzer** above the list.

6. This tool contains a wealth of information and is very easy to use. First of all, you will see a box containing several bubbles, within each of which will be a name. These are the domain names with which the user most frequently communicates. The larger the bubble, the more often emails are sent to and from people at these domains. This can especially be of interest in instances of intellectual property fraud, or when investigating disgruntled employees. Clicking on any one of these bubbles will make lines appear between them. These lines demonstrate how many messages have been sent and received between different domains. The thickness of the line indicates the amount of traffic between the domains.

   You can then expand the domain names to see a list of individual users. Hovering over a specific user will show their email address. You will also see more bubbles popping up around the individual user - like with the earlier example of domains, these bubbles show which individuals this user has emailed. Once again, the size of the bubble indicates the level of connection. If you want to exit the Social Analyzer tool and continue working on the case based on data you have found there, you can click **Post Results Back** on the left-hand side of the screen and then check **Label** in the pop-up box that appears. This will label all the emails you have been looking at, so that when you navigate back to your main case view you will be able to sort data based on this.

7. Internet history is another popular source of forensic information, and FTK's Visualization tool has several options here as well. It covers all the most popular browsers and once again lets you put data from this into a timeline and then drill down to more specific points of interest. However, you can only view data from one browser at a time. In the case you have loaded, go to **Evidence | Additional Analysis | Evidence Processing** and select **Process Internet Browser History for Visualization**. This will bring up a timeline. Once you are in the Timeline view, you can navigate around it in exactly the same way you would with email data, by clicking on individual dates and items to drill down into the details. Again, you can label items by selecting them from the list and then clicking **Mark Selected Items** on the right-hand side of the screen. This will allow you to label them so that you can access them within the main case.

8. Geolocation data can provide a wealth of useful information and opportunities for further investigation, and it has the added bonus of being easy to understand even for a non-technical client. Geolocation is automatically turned on in FTK cases, however you must be connected to the internet in order to access it. For this reason, it may be worth shutting down a live case you are working on and opening a duplicate one in order to prevent potential contamination of data. Once you have selected the **Geolocation** tab, you will be able to see your data spread across the world. You can then drill down into a specific region by clicking on the bubble over the country or area you would like to examine. Clicking on a bubble will zoom in on the map and show you specific points of interest. You can then click on one of the points to see details about what happened in this location. After selecting your specific location, you can right-click on it, which will bring up several options. These will allow you to change the color of the pin or change it to an icon, view the precise location in longitude and latitude, and mark the location either by labeling it or creating a bookmark. Once again, any labels added can then be processed back in the main case.

How it works...

The visualization tool works by using a graphical interface to highlight important elements within a case. It structures these either by time or by location, depending on the preferences set by the user.

Drilling down within the visualization tool allows for extra analysis of the dataset, and also enables the user to mark specific items of interest which can then be reviewed within the main case.

Making a timeline in Autopsy

Autopsy is a popular piece of open source freeware with many advocates in the digital forensics community. The tool performs all the basic functions required for investigative work, and also makes it easy for technical users to extend it by creating compatible plugins.

The timeline feature is generally loaded within a case that is already running, and ideally needs to have several options enabled in order to be used efficiently, these being:

- Hash lookup with NSRL
- Recent activity
- EXIF data

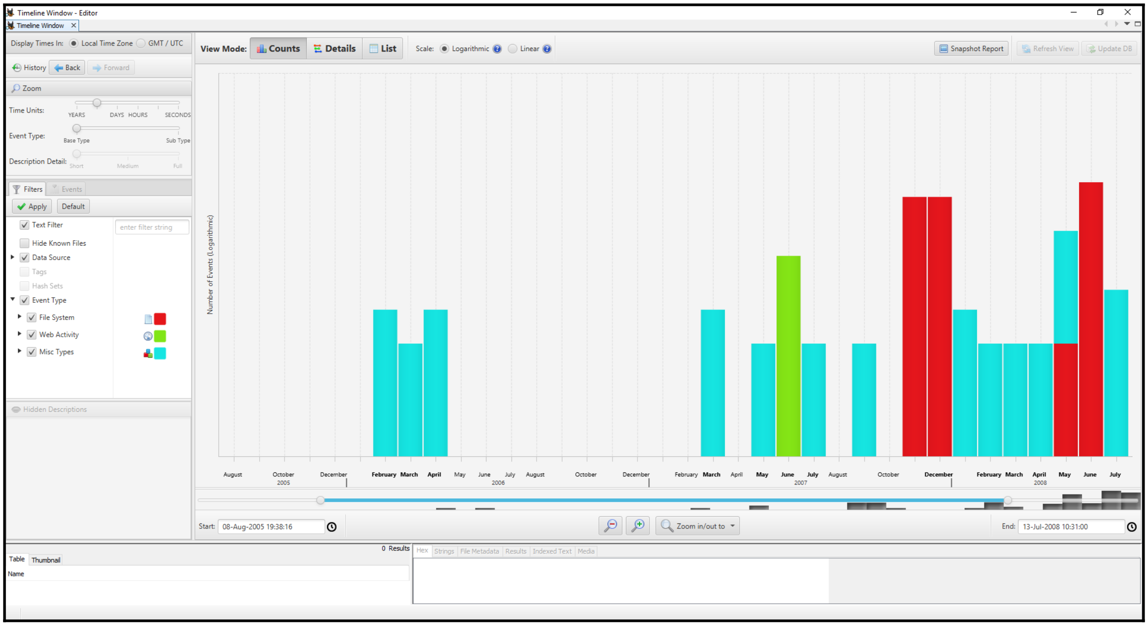
Getting ready

First, load up your case in Autopsy and then click **Timeline** at the top of the page. A new window will now open, which will give you access to the Timeline feature.

Although Autopsy's Timeline feature does not have as many bells and whistles as FTK's Visualization tool or Nuix's Web Review & Analytics add-on, it is nonetheless a great starting point for drilling down into digital forensic data.

How to do it...

At first glance, you will see a bar graph which shows the number of things that have taken place each year. Clicking on a given year will break that period down into months; clicking on a particular month will break the timeline down into days; then, finally, clicking on days will bring you an hour-by-hour timeline view. There are currently no more granular levels than this. The following image shows a timeline broken down by month:



Display Times In: ● Local Time Zone ○ GMT / UTC

View Mode: Counts

Scale: ● Logarithmic ○ Linear

☑ Text Filter

□ Hide Known Files

☑ Data Source

□ Tags

□ Hash Sets

☑ Event Type

☑ File System 🟥

☑ Web Activity 🟩

☑ Misc Types 🟦

Start: 08-Aug-2005 19:38:16

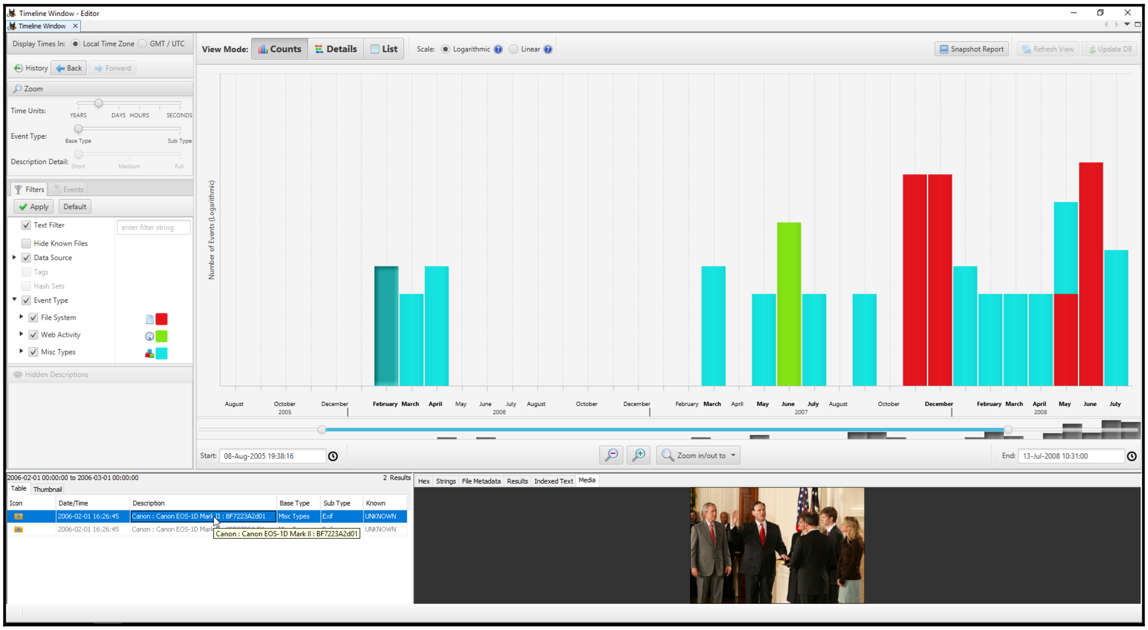
End: 13-Jul-2008 10:31:00

0 Results

Fig. 11.1. The timeline view in Autopsy

The procedure to prepare a timeline in Autopsy:

1. Once you have chosen your time period, you will be able to visualize any relevant data in the bottom left-hand corner of the screen. Here you will see a list of items of interest; precisely what is shown there will depend on the options you selected when you loaded your case. Clicking on any one of these listed items will generate a preview in the pane in the bottom right of the screen, as shown in the following figure:



Timeline Window - Editor

Display Times In: ● Local Time Zone ○ GMT / UTC

View Mode: Counts | Details | List

Scale: ● Logarithmic ○ Linear

☑ Text Filter
☐ Hide Known Files
☑ Data Source
☐ Tags
☐ Hash Sets
☑ Event Type
☑ File System 🟥
☑ Web Activity 🟩
☑ Misc Types 🟦

Start: 08-Aug-2005 19:38:16

End: 13-Jul-2008 10:31:00

2006-02-01 00:00:00 to 2006-03-01 00:00:00 — 2 Results

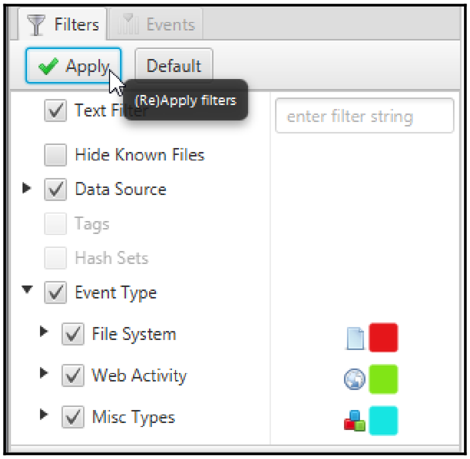
Icon	Date/Time	Description	Base Type	Sub Type	Known
	2006-02-01 16:26:45	Canon : Canon EOS-1D Mark II : BF7223A2d01	Misc Types	Exif	UNKNOWN
	2006-02-01 16:26:45	Canon : Canon EOS-1D Mark			UNKNOWN

Canon : Canon EOS-1D Mark II : BF7223A2d01

Fig 11.2. The preview panel will show up in the bottom right of the screen

Clicking on the line separating the preview and list panes from the timeline view above will allow you to resize the previews.

2. To the left of the screen, in the main timeline view, you will see several options. These allow you to tell Autopsy what it is you are particularly interested in uncovering within your case. Selecting any number of these options will mean that Autopsy will automatically color code them and add them to the timeline view, as shown in the following screenshot:



☑ Text Filter

□ Hide Known Files

☑ Data Source

□ Tags

□ Hash Sets

☑ Event Type

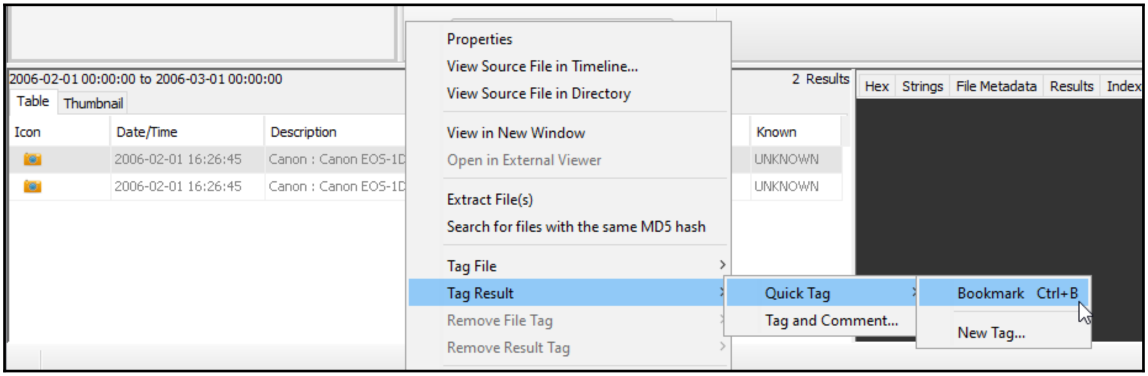
☑ File System 🟥

☑ Web Activity 🟩

☑ Misc Types 🟦

Fig 11.3. Applying filters to a timeline

3. Once you have found your items of interest, you can right click on them within the list pane and go to **Tag Result,** which will then allow you to give them a tag of your choice, as shown in the following screenshot:



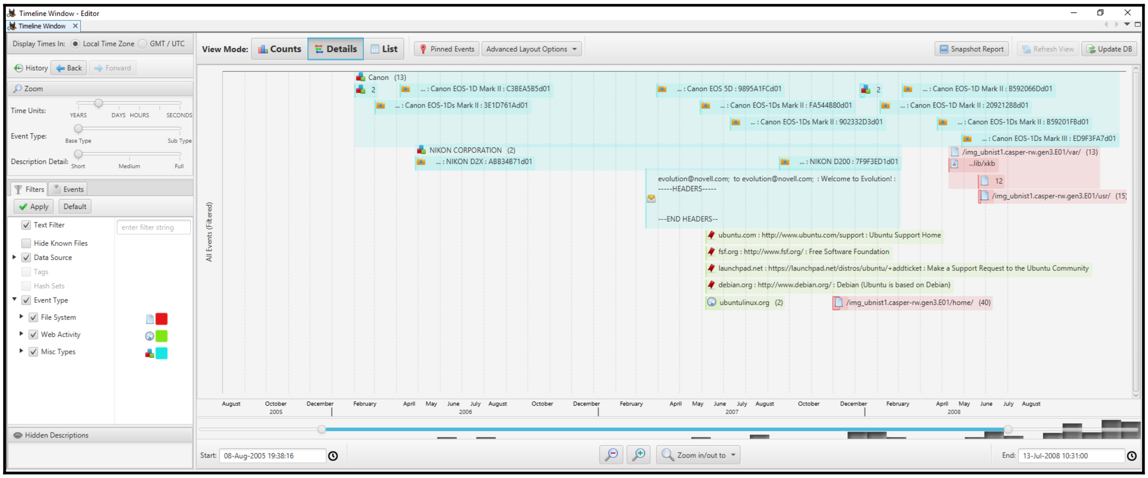
2006-02-01 00:00:00 to 2006-03-01 00:00:00

2 Results

Icon	Date/Time	Description	Known
	2006-02-01 16:26:45	Canon : Canon EOS-1D	UNKNOWN
	2006-02-01 16:26:45	Canon : Canon EOS-1D	UNKNOWN

Fig 11.4. Tagging results in a timeline

4. Looking along the top of the screen, you will see three options next to **View Mode**: Counts, Details, and List. Clicking **Details** will show a different view of the timeline, with horizontal rather than vertical bars, and with added details regarding each item, as shown in the following screenshot:



Display Times In: ● Local Time Zone ○ GMT / UTC

Time Units:

Event Type:

Description Detail:

☑ Text Filter enter filter string

□ Hide Known Files

☑ Data Source

□ Tags

□ Hash Sets

☑ Event Type

☑ File System 🟥

☑ Web Activity 🟩

☑ Misc Types 🟦

Canon (13)

2

... : Canon EOS-1D Mark II : C3BEA5B5d01

... : Canon EOS-1Ds Mark II : 3E1D761Ad01

... : Canon EOS 5D : 9895A1FCd01

... : Canon EOS-1Ds Mark II : FA544B80d01

... : Canon EOS-1Ds Mark II : 902332D3d01

2

... : Canon EOS-1D Mark II : B592066Dd01

... : Canon EOS-1D Mark II : 20921288d01

... : Canon EOS-1Ds Mark II : B59201FBd01

... : Canon EOS-1Ds Mark III : ED9F3FA7d01

NIKON CORPORATION (2)

... : NIKON D2X : ABB34B71d01

... : NIKON D200 : 7F9F3ED1d01

/img_ubnist1.casper-rw.gen3.E01/var/ (13)

...lib/xkb

12

/img_ubnist1.casper-rw.gen3.E01/usr/ (15)

evolution@novell.com; to evolution@novell.com; : Welcome to Evolution! :
-----HEADERS-----

---END HEADERS--

ubuntu.com : http://www.ubuntu.com/support : Ubuntu Support Home

fsf.org : http://www.fsf.org/ : Free Software Foundation

launchpad.net : https://launchpad.net/distros/ubuntu/+addticket : Make a Support Request to the Ubuntu Community

debian.org : http://www.debian.org/ : Debian (Ubuntu is based on Debian)

ubuntulinux.org (2)

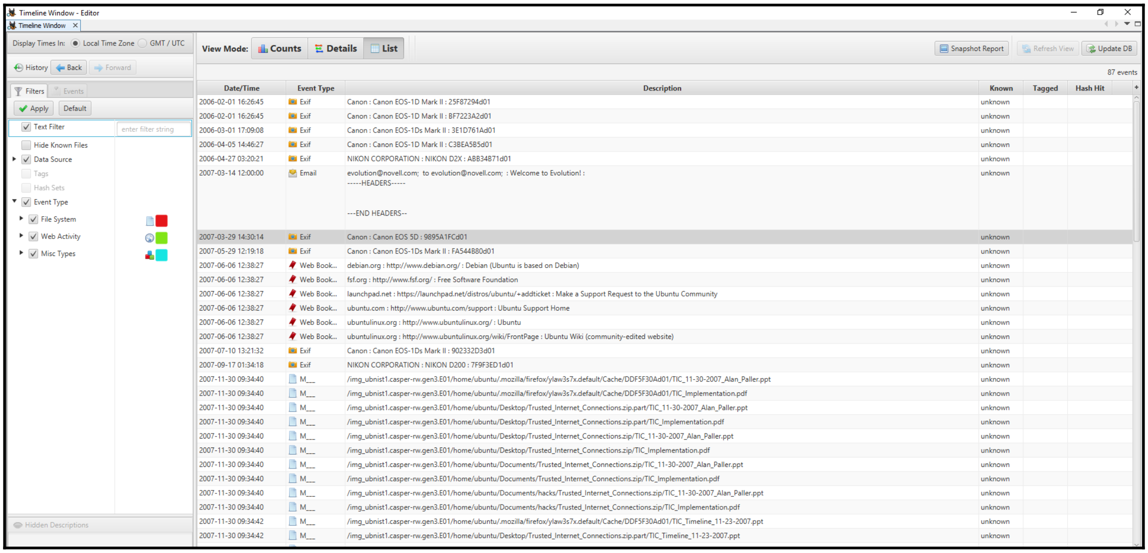
/img_ubnist1.casper-rw.gen3.E01/home/ (40)

Start: 08-Aug-2005 19:38:16

End: 13-Jul-2008 10:31:00

Fig 11.5. The **Details** view in Timeline

5. Likewise, the **List** pane will show the data in a vertical list, without any kind of graphical interface. This can be useful as it still arranges data by time frame, but it is more detailed and can be easier to sort, as shown in the following screenshot:



Date/Time	Event Type	Description	Known	Tagged	Hash Hit
2006-02-01 16:26:45	Exif	Canon : Canon EOS-1D Mark II : 25F87294d01	unknown		
2006-02-01 16:26:45	Exif	Canon : Canon EOS-1D Mark II : BF7223A2d01	unknown		
2006-03-01 17:09:08	Exif	Canon : Canon EOS-1Ds Mark II : 3E1D761Ad01	unknown		
2006-04-05 14:46:27	Exif	Canon : Canon EOS-1D Mark II : C3BEA5B5d01	unknown		
2006-04-27 03:20:21	Exif	NIKON CORPORATION : NIKON D2X : ABB34B71d01	unknown		
2007-03-14 12:00:00	Email	evolution@novell.com; to evolution@novell.com; : Welcome to Evolution! : -----HEADERS----- ---END HEADERS--	unknown		
2007-03-29 14:30:14	Exif	Canon : Canon EOS 5D : 9895A1FCd01	unknown		
2007-05-29 12:19:18	Exif	Canon : Canon EOS-1Ds Mark II : FA544B80d01	unknown		
2007-06-06 12:38:27	Web Book...	debian.org : http://www.debian.org/ : Debian (Ubuntu is based on Debian)	unknown		
2007-06-06 12:38:27	Web Book...	fsf.org : http://www.fsf.org/ : Free Software Foundation	unknown		
2007-06-06 12:38:27	Web Book...	launchpad.net : https://launchpad.net/distros/ubuntu/+addticket : Make a Support Request to the Ubuntu Community	unknown		
2007-06-06 12:38:27	Web Book...	ubuntu.com : http://www.ubuntu.com/support : Ubuntu Support Home	unknown		
2007-06-06 12:38:27	Web Book...	ubuntulinux.org : http://www.ubuntulinux.org/ : Ubuntu	unknown		
2007-06-06 12:38:27	Web Book...	ubuntulinux.org : http://www.ubuntulinux.org/wiki/FrontPage : Ubuntu Wiki (community-edited website)	unknown		
2007-07-10 13:21:32	Exif	Canon : Canon EOS-1Ds Mark II : 902332D3d01	unknown		
2007-09-17 01:34:18	Exif	NIKON CORPORATION : NIKON D200 : 7F9F3ED1d01	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/.mozilla/firefox/ylaw3s7x.default/Cache/DDF5F30Ad01/TIC_11-30-2007_Alan_Paller.ppt	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/.mozilla/firefox/ylaw3s7x.default/Cache/DDF5F30Ad01/TIC_Implementation.pdf	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip.part/TIC_11-30-2007_Alan_Paller.ppt	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip.part/TIC_Implementation.pdf	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip/TIC_11-30-2007_Alan_Paller.ppt	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip/TIC_Implementation.pdf	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/Trusted_Internet_Connections.zip/TIC_11-30-2007_Alan_Paller.ppt	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/Trusted_Internet_Connections.zip/TIC_Implementation.pdf	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/hacks/Trusted_Internet_Connections.zip/TIC_11-30-2007_Alan_Paller.ppt	unknown		
2007-11-30 09:34:40	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Documents/hacks/Trusted_Internet_Connections.zip/TIC_Implementation.pdf	unknown		
2007-11-30 09:34:42	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/.mozilla/firefox/ylaw3s7x.default/Cache/DDF5F30Ad01/TIC_Timeline_11-23-2007.ppt	unknown		
2007-11-30 09:34:42	M___	/img_ubnist1.casper-rw.gen3.E01/home/ubuntu/Desktop/Trusted_Internet_Connections.zip.part/TIC_Timeline_11-23-2007.ppt	unknown		

Fig 11.6. The List view is the most detailed

Data can then be exported in HTML, as an Excel document, or as a `TSK` file. The timeline itself will not show up automatically in a report, so if you want this to be included you will have to screenshot it and add it in manually later on.

How it works...

Autopsy's Timeline feature is essentially a stripped-back version of the timeline tools included in commercial forensic suites. It works by analyzing the data within the case you have entered, and then arranging that data within a given time period.

Because Autopsy is an open source tool, it is possible to create your own add-ons which may be helpful in bespoke investigative circumstances.

See also

The Autopsy download page: `http://sleuthkit.org/autopsy/download.php`
The Autopsy user guide: `http://sleuthkit.org/autopsy/docs/user-docs/3.1/`

Sometimes a case is more complex than simply uncovering data from a single source and reporting back on it. Particularly in law enforcement investigations, there will often be many different people working on the same case, some of whom are non-technical investigators, and this makes it important for multiple individuals to be able to view, sort through, and report back on data regardless of their level of technical knowledge.

Nuix's solution to this is its Web Review & Analytics tool, which sits on top of its eDiscovery and Director suites and allows multiple users to collaborate.

Getting ready

Assuming you already have a Nuix license, you can get this as an add-on from Nuix's website, the address of which is provided at the end of this chapter.

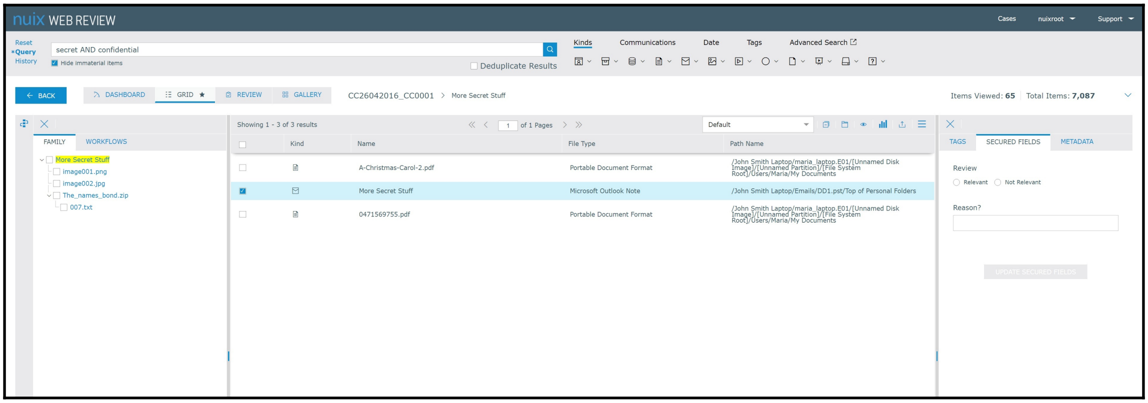
First of all, create your case in a Workbench as usual and open your evidence items. Once you have all the data you require, open Web Review & Analytics, navigate to your case, and open it.

How to do it...

What you will see next depends upon your level of permissions. All users are initially taken by default to their Dashboard. For administrators, this will show a list of users along with checkboxes describing their permissions, which can be managed and changed in this view.

For non-administrative users, the Dashboard will show an overview of cases. Click on one of these to begin.

1. Once your case is loaded, you can search for specific keywords or terms of interest using the bar along the top. This will bring back a list of results in the centre pane, from which you can then drill down further, as shown in the following screenshot:



secret AND confidential

☑ Hide immaterial items

□ Deduplicate Results

CC26042016_CC0001 > More Secret Stuff

Items Viewed: **65** | Total Items: **7,087**

More Secret Stuff
- image001.png
- image002.jpg
- The_names_bond.zip
  - 007.txt

Showing 1 - 3 of 3 results — 1 of 1 Pages — Default

□	Kind	Name	File Type	Path Name
□		A-Christmas-Carol-2.pdf	Portable Document Format	/John Smith Laptop/maria_laptop.E01/[Unnamed Disk Image]/[Unnamed Partition]/[File System Root]/Users/Maria/My Documents
☑		More Secret Stuff	Microsoft Outlook Note	/John Smith Laptop/Emails/DD1.pst/Top of Personal Folders
□		0471569755.pdf	Portable Document Format	/John Smith Laptop/maria_laptop.E01/[Unnamed Disk Image]/[Unnamed Partition]/[File System Root]/Users/Maria/My Documents

Review

○ Relevant ○ Not Relevant

Reason?

Fig 11.7. A list of results loaded in Nuix's Web Review & Analytics

Clicking on any of the items in the search results will allow you to view them in more detail. A preview of the item in question will show up in the center of the screen, and along the right-hand side you will see three tabs: **TAGS**, **SECURED FIELDS**, and **METADATA. METADATA** which allows you to view either the metadata associated with a specific item, or the information that has been associated with it by other users of Web Review & Analytics.

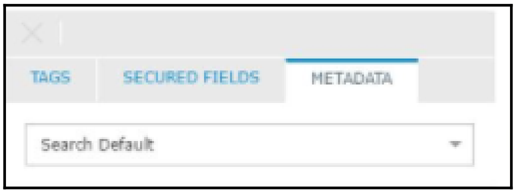


Fig 11.8. Viewing options in Web Review & Analytics

2. Clicking on **Kinds** at the top of the screen will bring up a list of options allowing you to sort data based on the type of file or its associated metadata. Looking for images, for example, will bring up a gallery view similar to what you see in most forensic software, with thumbnail-sized previews of images that can then be selected, tagged, commented on, or analyzed further.
3. Selecting geolocation will bring up a map with pins in each location relevant to the case. Clicking on any of these pins will allow you to zoom in and see which data source is linked to this location. Geolocation data is shown in Google Maps, a familiar interface for most users, as shown in the following screenshot:

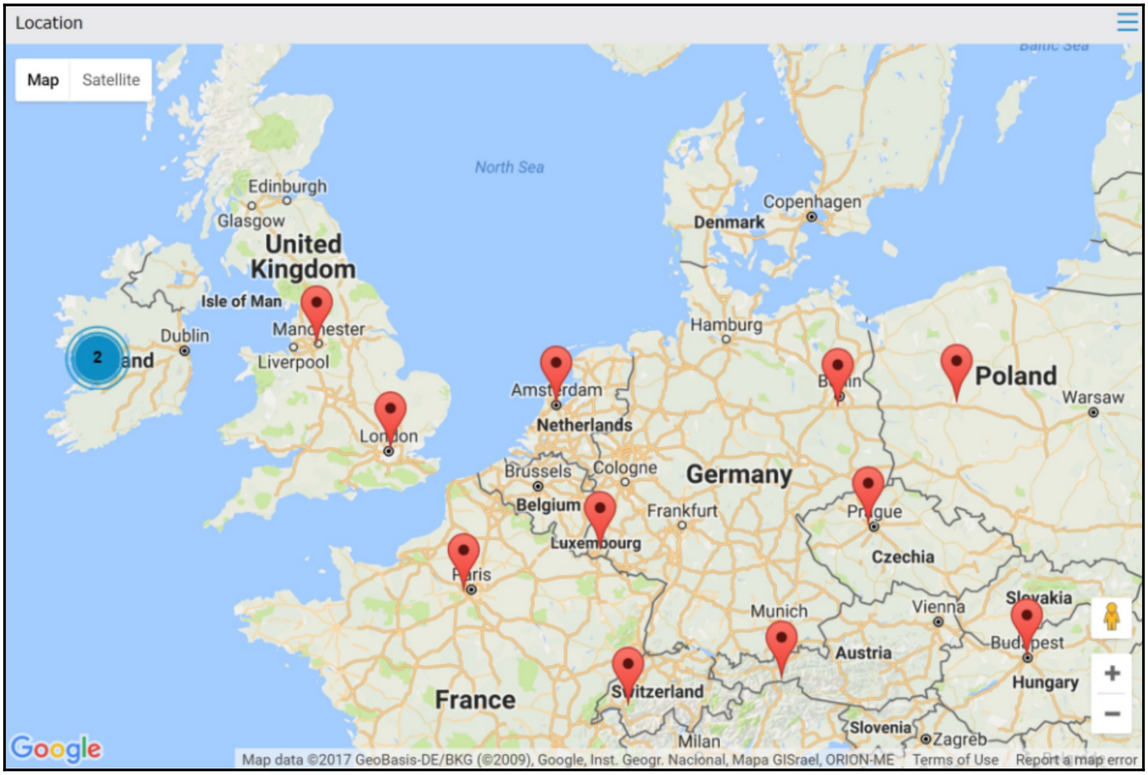


Fig 11.9. Google Maps geolocation data in Nuix WR&A

4. One neat feature of Nuix's Web Review & Analytics tool is its ability to create individual metadata profiles. If you are working as part of a team, for example, and one person deals with images while another is tasked with analyzing all data from a particular mobile device, you can easily create a metadata profile for each of these users, leading to fewer problems with cross-contamination of data and aiding in triage. To create an individual metadata profile, simply click **Global Options** at the top of the screen, select **Create a metadata profile**, and follow the instructions to set it up.
5. The reporting section within Web Review & Analytics is particularly useful, due to its usability both in terms of being able to drill down into the details, and being accessible for non-technical users. The graphs and charts are easy to read, and each one can be clicked for more information, which will then take a user back to the Grid view and allow them to deep dive into the results. In the following example, the user has told Nuix Web Review & Analytics to show a list of languages, which is a built-in feature. The tool can detect which languages are being used throughout a dataset and then structure these into an easy-to-read graph such as the following one. This allows users to break data down into individual components which can then be looked at further.

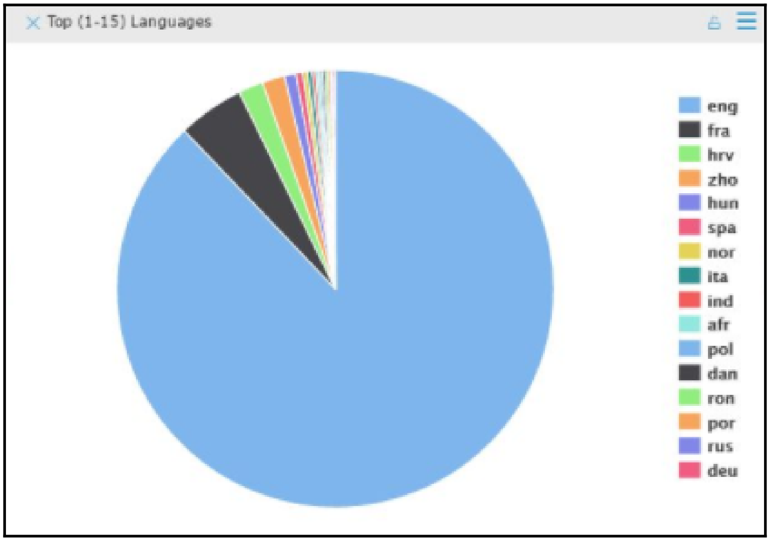


Fig 11.10. Web Review & Analytics features interactive graphs

Reports can be downloaded as PDFs or a variety of other common file types. However, one of the most popular ways of reporting in Web Review & Analytics is by simply creating a new user with no administrative privileges and only the ability to view, rather than to manipulate, the data within the case. That way, a client or customer can log into Web Review & Analytics and view in detail the specific items that interest them the most.

How it works...

Nuix's Web Review & Analytics works by taking a web-based interface concept and applying this to large-scale digital forensic investigations. This makes it easier to triage large cases, to avoid accidental cross-contamination of data and preserve the chain of custody, and to keep track of who is working on which part of a case.

See also

Nuix's Web Review & Analytics: `https://www.nuix.com/products/nuix-web-review-analytics`(accessed 13/07/17).

12

Troubleshooting in Windows Forensic Analysis

In this chapter, we will cover the following recipes:

- Troubleshooting in commercial tools
- Troubleshooting in free and open source tools
- Troubleshooting when processes fail
- False positives during data processing with digital forensics software
- Taking your first steps in digital forensics
- Advanced further reading

Introduction

We would all like our cases to be one hundred percent perfect all the time, but unfortunately things do go wrong sometimes. Whether it's because of a technical fault with a product you're using, a mistake made by an investigator, a faulty dataset in the first place, or some kind of legislative issue encountered when a case goes to court, it is all too common to come up against obstacles in your investigations.

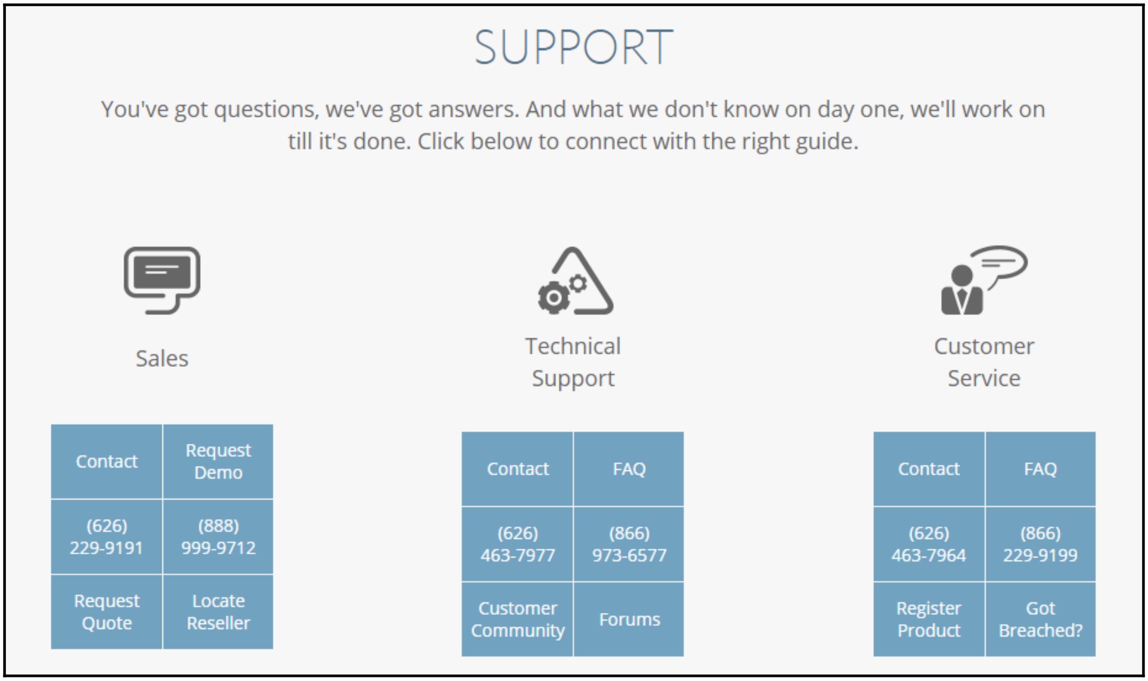
In this chapter, we highlight some of the most common things that can go wrong with popular forensic suites and how to fix them. We will then take a look at what you can do when processes fail, and when you come up against legislative or jurisdictional challenges.

Finally, we will provide you with a short guide to taking your first steps in digital forensics, and recommend some advanced further reading - if you haven't been put off yet!

Troubleshooting in commercial tools

Digital forensics is a very complex field. This means that you are likely to face different problems while working on your cases. Problems may be of different natures: you could fail to install a tool because your workstation doesn't have additional third-party software (usually it's included in the package by the developers); you could fail to process the data source properly because it's damaged or the format or file system is unsupported; you could fail to parse some forensic artifacts because their format has been changed and isn't supported by your piece of software yet, and so on.

Thanks to the developers of commercial forensic software, including EnCase, FTK, AXIOM, Evidence Center, Intella, and so on, you can solve almost any problem quickly and easily (most of the time) with the help of their customer support services, which are usually included in your licence. All you need to do is write an email to the support team, or even call them.



SUPPORT

You've got questions, we've got answers. And what we don't know on day one, we'll work on till it's done. Click below to connect with the right guide.

Sales

Contact	Request Demo
(626) 229-9191	(888) 999-9712
Request Quote	Locate Reseller

Technical Support

Contact	FAQ
(626) 463-7977	(866) 973-6577
Customer Community	Forums

Customer Service

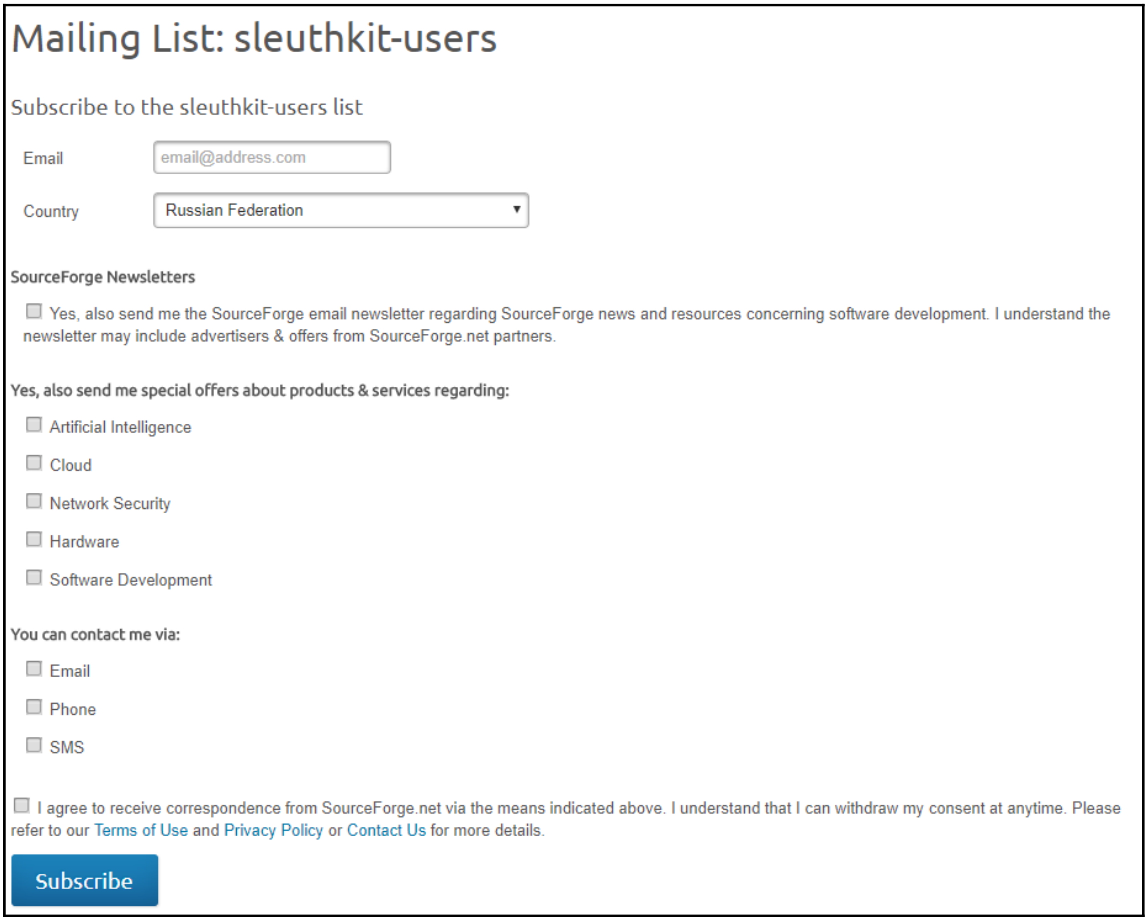
Contact	FAQ
(626) 463-7964	(866) 229-9199
Register Product	Got Breached?

Figure 12.1. Guidance Software EnCase Forensic support contacts

Troubleshooting in free and open source tools

Of course, free and open source tools don't have customer support services, but they have developers. Often, you can contact the developer directly and ask your questions, or even share (if possible) the data source problems you have with them. This helps developers to improve their tools and help the community.

Some tools, such as The Sleuth Kit and Autopsy for example, have mailing lists: you can ask your question and the developer or active users will answer it, as shown in the following screenshot:



Mailing List: sleuthkit-users

Subscribe to the sleuthkit-users list

Email email@address.com

Country Russian Federation

SourceForge Newsletters

□ Yes, also send me the SourceForge email newsletter regarding SourceForge news and resources concerning software development. I understand the newsletter may include advertisers & offers from SourceForge.net partners.

Yes, also send me special offers about products & services regarding:

□ Artificial Intelligence

□ Cloud

□ Network Security

□ Hardware

□ Software Development

You can contact me via:

□ Email

□ Phone

□ SMS

□ I agree to receive correspondence from SourceForge.net via the means indicated above. I understand that I can withdraw my consent at anytime. Please refer to our Terms of Use and Privacy Policy or Contact Us for more details.

Figure 12.2. Subscribing to the sleuthkit-users list

Troubleshooting when processes fail

Since investigative and judicial processes are put together by humans, from time to time they fail; sometimes quite spectacularly. In this section, we will look at a couple of common examples and discuss what to do when situations like these arise.

Soundness of evidence

One of the most frequent criticisms levelled at digital forensic investigators comes in the form of a challenge to the soundness of the evidence they are presenting. This includes the common *It wasn't me* defense, wherein a defendant insists that they were not the one using the device in question; the suggestion that the evidence itself is somehow faulty; either because of a virus or malware having infected a device before it was analysed, or because the process of analysis itself has modified the data in some way.

There are a couple of ways to deal with these concerns, so let's take a look at them one by one.

It wasn't me

One of the most difficult challenges to deal with in digital forensic investigations is the defense that someone else must have been using a device when a crime or other nefarious activity occurred. It is a favorite among defendants around the world.

It is almost always impossible to definitively prove that a specific individual was the one using a particular device at a given time. However, in most courts of law and certainly in civil cases, all the investigator is required to do is demonstrate that this is the case beyond reasonable doubt. Sure, someone else could have broken into the defendant's house, guessed their password, and downloaded some indecent images of children onto their machine when they were out shopping for their elderly mother, but the likelihood of this is rather remote. This is an extreme example, but it does illustrate the point: most of the time, the user who actually owns the device is the person using it.

In cases where this is a little more difficult to prove—for example, when evidence is admitted from a machine which is shared by several people who live in the same household—there are sometimes other ways to prove beyond reasonable doubt that a particular person was the one accessing the device at that time.

Some useful questions to consider in such a case include:

- Did the user's behavior model that of a specific person within the household during the time the activity in question was taking place? For example, which tabs had recently been opened online? Were they checking a particular email account or social profile?
- If looking at a text-based document, does the language used correspond to the normal speech and writing patterns of the individual in question? Are they using words they commonly use in their other documents? Are some of the same words misspelled when you compare the document with messages you know they have sent?
- Can data from other devices help to establish the presence or absence of other household members at the time the activity took place?

So for example, let's say that one member of a household is accused of downloading illegal files from the internet. Person A is your most likely suspect, because it is their account that was logged in when the downloads occurred.

However, you might not have caught the person red-handed, so you will need to look for other data sources in order to demonstrate beyond any reasonable doubt that it was them. Let's say the desktop computer in question is used by several members of the household, and each has their own account. Showing which account logged in would be the first step toward proving who downloaded the files.

At this point, the defendant may say that someone else must have used their account; perhaps they accidentally left it logged in, or perhaps someone guessed or knew the password.

Guessing the password is always a possibility, but another person's writing style is much harder to fake, so this is where you can bring in the other questions that were listed above. Firstly, look at the language used by the person who downloaded the files. Did they run any related searches before the downloads occurred, and if so, do the search terms contain any linguistic markers that may prove useful?

Generally, by this point, you will have demonstrated beyond a reasonable doubt that your defendant is guilty. But, for the sake of argument, let's say your defendant is very insistent that they were not using the computer. No matter how much evidence you present to them, they never admit to a word you say, and continue to say *It wasn't me*.

You may now want to look at evidence gathered from the other people in the household, to see whether data from their devices can establish that none of them downloaded the files.

Luckily, the booming internet of things industry is making such data increasingly easy to collect. Let's say you have managed to seize every device in the house, and you have the datasets in front of you. You look through them in the Timeline views we discussed in `Chapter 11`, *Data Visualization*, and you narrow down your investigation to the time when the files were being downloaded.

Now you can discover what each household member was doing at a given time. Let's say that person B in the house does all the cooking, and at the time the messages were sent, the **Amazon Echo** was on the counter in the kitchen, talking through a recipe for beef bourguignon. Data from the smart TV shows that someone was sitting on the sofa watching a movie, and this is backed up by data from person C's smartphone, which was being used idly to Google names of the actors who were appearing on the screen.

Data from person D's Fit Bit places them in the shower at the time the messages were being sent, and person E has been caught on camera live-streaming a makeup tutorial to their followers on YouTube.

This leaves person A as the most likely suspect. But of course, a defendant may still continue to insist it wasn't them.

It was a virus / I was hacked

Sometimes, a defendant will move from one defense to another, in a kind of cascading avalanche of desperation. Let's stick with our example above. Having established that it must have been person A at the computer when the files were downloaded, they have now come up with a new defense: it still wasn't them because, although they were using the device, they didn't deliberately download the files. So either the machine must have a virus, or they might have been hacked.

In today's world it can be difficult to establish that a device had no viruses. Alongside the usual challenges with trying to prove a negative, investigators also come up against increasingly intelligent malware which can cover its tracks, overwrite logs, and delete itself from systems with barely a trace.

In most cases, however, you can use a few methods to establish the likelihood that a virus is present on a machine.

Firstly, and most importantly, run a scan. Unless you are working a particularly complex case, most malware will show up in an initial scan, and once you know what it is, you will be able to work out what it can and cannot do. Also, check whether the machine has antivirus software, and if so, whether it is up to date.

Secondly, if your investigation is focused on a specific time frame, as in our current example, look at what else was happening on the machine at that time. If someone was sending messages in one tab while illegal files were being downloaded in another, it is highly unlikely that they did not know about it. Likewise, it is unlikely that a virus would have navigated to a website, downloaded P2P software, given the computer permission to install said software, clicked through all the options, agreed to the terms and conditions, opened the software, and then used it to download images.

Your process is faulty

A much more serious defense is when a person claims that the investigator's process was faulty. They may claim, for example, that the evidence was contaminated; that their case was unfairly handled; that their rights were not upheld; or that crucial data was skipped, among other things.

The most efficient way to troubleshoot against such things happening is to take precautions to make sure you do not come up against them in the first place. Arguably, the most important of these is establishing and maintaining a proper chain of custody.

A chain of custody is essentially the paperwork that shows where the evidence you have collected has been, how long it has been there, and who was responsible for it. So if you are working in a team of investigators, your chain of custody documentation should detail who attended the scene, who viewed the devices at the scene and decided whether to remove them or not, how were they handled when they were removed (for example, were they shut down and unplugged, or were they already switched off when they were found), how they got to the processing area, who was responsible for them during that time, and who was ultimately responsible for analyzing the data.

Other important details to note include any actions that were taken on the device, for example:

- At which point did you take a forensic image of the device?
- Did you back up the original device? At what point did you do so, and where was this backup stored?
- How was the device transportation handled? For example, was it put in a Faraday bag?
- Which tools did you use to examine the device, and how did you determine that they were working correctly?

If you can answer all of the questions above, and you have accurately filled in your chain of custody document, your defendant will be hard-pressed to argue a fault in your process.

Legal and jurisdictional challenges

Probably the most difficult challenges to come up against in an investigation are legal and jurisdictional constraints.

Perhaps you have gathered evidence that implicates a specific website, the server of which is in a country which has no reciprocal agreement with your own. Perhaps data is stored on the cloud and its legal jurisdiction is unclear. Perhaps you have compiled a case against a suspect, but they are in another jurisdiction and you have no authority there.

Ultimately, we all have to work within the boundaries of the law. While popular culture may show digital forensic experts illegally hacking into suspects' computers and breaking all sorts of rules to make sure their case reaches a conviction, in the real world this is not a possibility.

If you do come up against a jurisdictional challenge, your best bet is to follow through with the relevant authorities as best you can. In cases involving serious crimes, for example child protection or drug trafficking investigations, there will often be a way to work with international law enforcement agencies to ensure that your case can be solved. This can take time and requires a lot of patience, however the end result is usually worth it.

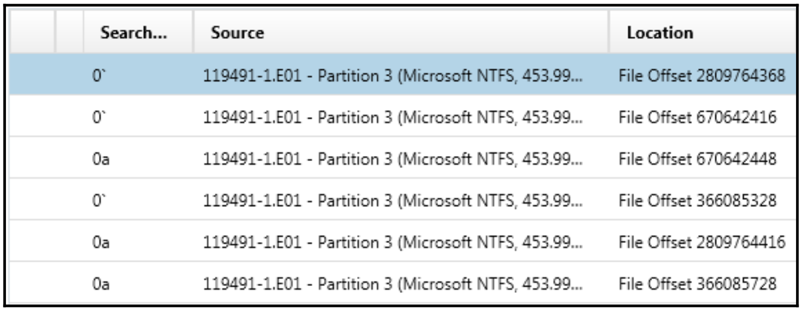
The main thing to bear in mind when it comes to legal challenges is that, tempting as it may be to cut a few corners when you know someone is committing a crime, this will only damage your investigation. Not only will your own reputation be put on the line, but your potential contamination of evidence may lead to a case being thrown out, thus having the opposite effect to the one you intended.

False positives during data processing with digital forensics software

During your computer forensic examination with different tools, both commercial and free or open source, you will face so-called *false positives*, especially if you are planning to use data carving techniques.

So why do we all face them? No, it's not bugs in your forensic software. The thing is, these false positives just match the criteria used by your piece of software to carve data from, for example, unallocated space of the hard drive or its forensic image.

You will most likely face false positives working with tools which support a large number of different apps, for example Magnet AXIOM. But you must understand, it's better to have a number of false positives than one false negative!



		Search...	Source	Location
		0`	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 2809764368
		0`	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 670642416
		0a	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 670642448
		0`	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 366085328
		0a	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 2809764416
		0a	119491-1.E01 - Partition 3 (Microsoft NTFS, 453.99...	File Offset 366085728

Figure 12.3. False positives in Magnet AXIOM

As you can see in the preceding figure, it's not difficult to identify such artifacts: they look messy and don't make any sense.

Anyway, you as a computer forensic examiner must analyze all of them thoroughly, because you can find valuable pieces of evidence even among false positives.

Taking your first steps in digital forensics

If you’ve read this far and you’re not yet a digital forensics practitioner but are thinking about it as a potential career path, congratulations! You’re looking at working in a growing industry with a wealth of opportunities and a lot of different areas to pursue.

Your next steps in digital forensics will depend how far along the journey you are right now, and what you'd ultimately like to get into.

Ask yourself the following questions:

- Do I like working on practical solutions with a physically interactive element, such as taking apart pieces of machinery to find out what’s wrong with them?
- Do I enjoy technical challenges, such as mind games, puzzles, video games, and technology?
- Do I prefer to work alone or as part of a team?

- Is it more important to me to earn a lot of money, or to work in an area where I feel like I'm making a difference?
- Would I rather be involved in actual investigations, or in research and development of tools?
- Which areas of digital forensics appeal to me the most?

Everyone's answers to these questions will be different. No one can choose the right path for you except you; and even then, we all get it wrong sometimes! One of the great things about working in digital forensics, however, is that so many of the skills are transferable. Once you have a skill set that includes technical investigation, research activities, and an ability to remain calm under pressure, you can apply this to all sorts of possible careers.

The three main strands of digital forensics work involve law enforcement, corporate work, and academia. Let's take a brief look at each of these to see which might suit you best.

Academia

Academic research is a highly demanding career path which tends to be lower paid than other areas of forensic work, but it can be very rewarding. Working in academic research often gives you the opportunity to discover new techniques, and uncover new trends within the field. Depending on your institution and funding body, you may be able to work with some of the latest technologies, for example looking at the newest generation of Internet of Things devices and how forensic data from these can be used in investigations.

Getting into academic research will require at least an undergraduate degree. Generally, people come to realise that this field is for them in the course of their early studies, staying on for a postgraduate qualification, and then ultimately looking for research teams and groups to join.

Corporate

Corporate forensics is without a doubt the highest-paid of all the routes into the field, but competition for places is fierce. However, digital forensics is a growing industry, so the number of jobs available is increasing all the time. The level of interest among jobseekers is also increasing, meaning that relatively few job openings exist.

Many digital forensics companies have several different branches: an investigative team that works on cases ranging from civil complaints to criminal lawsuits; a research and development team that comes up with software solutions to speed up these investigations; a sales and marketing team that takes these solutions and sells them to clients, the list goes on and on.

If you have a degree in computer forensics or a related field, you're already well on the way to being qualified for a position like this. However, many companies are looking for people who really stand out from the crowd. Securing an internship remains one of the best ways to end up with a job in the field. It is also worth looking into training options - many of the larger forensic companies, such as Guidance Software, AccessData, and Nuix, run their own training courses which give students a grounding in digital forensic techniques. Having one or more of these on your CV can help you stand out and demonstrate to employers your dedication to the field.

Law enforcement

One of the main reasons people give for going into the law enforcement side of digital forensics is wanting to make a difference. As a member of a police force or government agency, you will be tasked with working on a huge range of assignments, from drug investigations to child protection cases. Nowadays, most law enforcement agencies have a specific department devoted to computer forensics, and again, the proliferation of devices means that this field is only increasing.

Working in law enforcement isn't for everyone; often the hours are long and the pay compares unfavourably to what you might earn working for a large company. But for a lot of people, the reward of knowing you have directly helped others is more than a sufficient trade-off.

How do I get started?

If you're just beginning to think about pursuing a career in this area, the first step is to do some research. There is a wealth of information out there to help you get started, and a lot of ways to practice on your own even before you join a course or start learning officially.

Take a look at some of the digital forensics websites and forums, where more experienced practitioners share their knowledge and are available to help you with questions. You can download free tools such as Autopsy and FTK Imager to practice with, and use either your own devices or test images found online to create and work through cases. All of this will be valuable experience for when you start studying or working in the field.

Also consider attending some digital forensics conferences nearby. Many of these give discounts for students, and several run competitions for students to submit posters to be displayed during the conference. Events like these are a great way to meet other people in the industry and start to build your network.

In the next section, we will recommend some resources to help you get started.

Advanced further reading

The following books and websites will prove useful to anyone with an interest in the digital forensics field.

Books

For an advanced, in-depth, yet accessible introduction to the topic, Eoghan Casey's *Digital Evidence and Computer Crime* is a must-read.

Other good general introductions to the subject area include:

- *Forensic Computing* by Anthony Sammes and Brian Jenkinson
- *The Basics of Digital Forensics* by John Sammons
- *File System Forensic Analysis* by Brian Carrier

For more in-depth reading on specific topics, you could try some of the following:

- *Practical Forensic Imaging: Securing Digital Evidence with Linux Tools* by Bruce Nikkel, for a discussion on why correct image acquisition processes are so important, and a how-to guide that includes a lot of free and open source options.
- *Practical Mobile Forensics* by Heather Mahalik and Rohit Tamma, for an introduction to the forensic analysis of mobile devices and a useful how-to guide.
- *Mobile Forensic Investigations* by Lee Reiber, for a remarkably in-depth look at the field of mobile forensics and how to conduct your own analyses.
- *Learning iOS Forensics* by Mattia Epifani and Pasquale Stirparo, for help with investigating iPhones and easy to follow step-by-step instructions.

- *Learning Android Forensics* by Rohit Tamma and Donnie Tindall, for those who want to specialize in Android devices, or just want to supplement their knowledge of the subject.
- *The Art of Memory Forensics* by Michael Hale Ligh and Andrew Case, for an introduction to memory forensics and a discussion of their Volatility tool and how to use it.

Websites

- **4n6ir** : `http://blog.4n6ir.com/` — a frequently updated repository of information about incident response and digital forensics
- **Between Two DFIRs** : `https://betweentwodfirns.blogspot.co.uk/` — focusing heavily on the information security side of computer forensics (DFIR stands for Digital Forensics and Incident Response), Andrew Swartwood's blog is a great resource for anyone looking to enter this area.
- **Binary Foray** : `https://binaryforay.blogspot.co.uk/` — a technical read for the more advanced practitioner, Binary Foray explores some of the latest techniques in digital forensics.
- **BlackBag Tech** : `www.blackbagtech.com/index.php/blog` — BlackBag's blog includes several ongoing series that take readers through some of the basics of digital forensics.
- **Blackmore Ops :** `www.blackmoreops.com` — a must-read for Linux aficionados, this will tell you everything you need to know about getting set up with Kali and will also take you through some of its forensic applications.
- **Cyber Forensicator :** `www.cyberforensicator.com` — a blog covering digital forensics news and research, updated daily.
- **DFIR Training** : `www.dfir.training` — a fantastic resource listing hundreds of training opportunities and tools.
- **Didier Stevens** : `https://blog.didierstevens.com/` — includes resources and updates in the fields of digital forensics, incident response, ediscovery, hacking, and computer security.
- **Forensic Focus :** `www.forensicfocus.com` — the largest online hub for the digital forensics community, featuring articles, reviews, interviews, and an active community forum.

- **Forensic Lunch** : `https://www.youtube.com/user/LearnForensics`— David Cowen's popular YouTube channel, which discusses all different aspects of digital forensic investigation.
- **Forensics Wiki** : `www.forensicswiki.org` — contains a wealth of information for digital forensic practitioners, along with a regularly updated resources section.
- **Hacking Exposed Computer Forensics Blog** : `www.hecfblog.com` — David Cowen's blog is not updated often, but the posts are worth waiting for: filled with in-depth explanations of each step of the process, they are both accessible and interesting, for new and advanced investigators alike.
- **Mac4n6** : `www.mac4n6.com` — a digital forensics blog with a specific focus on Apple products.
- **Magnet Forensics** : `www.magnetforensics.com/blog/` — the blog of this digital forensics company frequently includes useful webinars, guides, and resources for practitioners. They often feature articles and webinars about child protection investigations.
- **Mobile & Technology Exploration**: `http://trewmte.blogspot.co.uk`— Greg Smith's blog covers several digital forensics topics, with a particular focus on mobile investigations.
- **Pro Digital 4n6:** `http://prodigital4n6.blogspot.co.uk/`—a blog discussing digital forensics and legal issues, with a number of useful case studies to illustrate points made.
- **This Week In 4n6:** `www.thisweekin4n6.com` — a weekly blog by Phill Moore, rounding up the latest news in digital forensics, ediscovery, and malware analysis.
- **Windows Incident Response:** `http://windowsir.blogspot.co.uk/` — Harlan Carvey's blog contains tips, how-to guides, and resources.
- **Zena Forensics:** `http://blog.digital-forensics.it/` — a collaborative effort from the team at RealityNet, this blog is not updated often, but does contain some interesting research and is worth keeping an eye on.

Twitter Accounts

- `@aboutdfir` — the creator of `aboutdfir.com` tweets industry news, investigations, and research
- `@binaryz0ne` — a digital forensics, incident response, malware, and traffic analysis researcher

- `@christammiller` — tweets research and views about digital forensics and incident response
- `@ForensicFocus` — the Twitter account of the popular website for digital forensics and ediscovery professionals
- `@Fr333k` — a researcher in computer security, online privacy, and digital forensics, tweeting the latest industry news
- `@grumpy4n6` — tweets about IT security, incident response, digital forensics, and malware
- `@hacks4pancakes` — a digital forensics and open source intelligence specialist who tweets about information security, computer forensics, and related topics
- `@HeatherMahalik` — a digital forensics professional and SANS instructor who tweets industry news on a regular basis
- `@icanhaspii` — a malware, ransomware, and information security professional tweets about digital forensics, incident response, and related subjects
- `@jayabaloo` — a specialist in network security architecture and VOIP security
- `@jessicambair` — tweets about cyber security, digital forensics, and incident response
- `@jeviscachee` — one of the authors of this book, who tweets about digital forensics, privacy, and computer security
- `@lept` — a member of the DigitalFIRE team at University College Dublin, tweeting digital forensics news and updates
- `@mrkscn` - a Fulbright scholar and digital forensics and cybersecurity Assistant Professor at University College Dublin, tweeting all the latest research and developments in the field
- `@NadiaShiyyab` — an IT, SCADA, and data cyber security researcher
- `@OlgaAngel` — a digital forensics and information security lecturer and researcher
- `@pstirparo` — a digital forensics, threat intelligence, and mobile security practitioner who tweets about all of these topics and more
- `@SuzanneWidup` — an author and researcher who tweets about digital forensics, data breaches, and *general geeky stuff*
- `@TroelsOerting` — the group CSO of Barclays Bank tweets about incident response, computer security, and digital forensics
- `@udgover` — tweets about computer forensics, programming, algorithms, and open source initiatives
- `@zaanpenguin` — an incident responder and digital forensic investigator who tweets industry news and interesting research

Index