Retrieving Digital Evidence: Methods, Techniques and Issues

Yuri Gubanov yug@belkasoft.com
Belkasoft Inc. http://belkasoft.com

Abstract

This article describes the various types of digital forensic evidence available on users' PC and laptop computers, and discusses methods of retrieving such evidence.

Introduction

A recent research conducted by Berkeley scientists concluded that up to 93% [1] of all information never leaves the digital domain. This means that the majority of information is being created, modified and consumed entirely in digital form. Most spreadsheets and databases never make it on paper, and most digital snapshots never get printed. There are many activities such as chats and social networking that are specific to digital and are even unimaginable outside of the virtual realm.

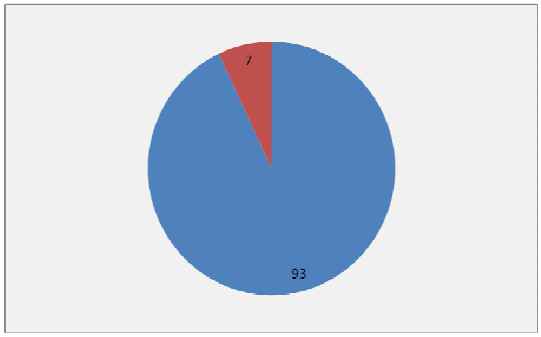

Figure 1: up to 93% of all information never leaves the digital domain

Most such activities leave definite traces, allowing investigators to obtain essential evidence, solve criminal cases and prevent crimes. This article discusses the many types of digital evidence produced by a typical computer user, criminal or not, and demonstrates methods and techniques available to extract that evidence out of the original PC and into the hands of a forensic investigator.

Table of Contents

Digital Forensics

It is hard to underestimate the importance of digital forensics. With many types of evidence being only available in a form of digital files stored on the computer's hard disk, getting access to this information is essential for today's investigations.

Instant Messengers

Instant Messengers became an important means of communication. Millions of people, regardless of their age, nationality, gender and computer skills, spend a lot of time using them every day. That's why more and more evidence can now be found in IM chat histories. To name a few, Live Messenger, ICQ, Yahoo! Messenger, AOL, Trillian, Skype, and Miranda IM are among the most commonly used. In China, QQ Messenger is very popular with almost a billion registered accounts.

Social Networking

Social networks are quickly becoming what 'traditional' instant messengers were just a few years ago. More and more communication is migrating from public chat rooms and private messengers into online social networks. Communications extracted from social networks can be extremely valuable to forensic investigators.

Web Browsers

Web browsing is a popular activity. Analyzing web browsing history, bookmarks, cached Web pages and images, stored form values and passwords gives keys to important evidence not available otherwise. Web browser cache may contain images with illicit content, as well as JavaScript-based malware that may be responsible for some suspicious-looking activities. Internet activities such as Google searches can be discovered and analyzed, often helping solve less than obvious crimes [4]. Dozens of different Web browsers exist beside the popular choice of Microsoft Internet Explorer, Mozilla Firefox and Chrome.

Email

Despite the raise of instant chats and social networks, email is still a major carrier of important information, which is especially true for corporate environments. With many online and offline email clients, it is too easy to overlook essential evidence without approaching it properly. Microsoft Outlook, Outlook Express, Windows Mail, Live Mail, Thunderbird, TheBat! and many other email applications are available on the market.

Peer-to-Peer and File Exchange Software

P2P and file exchange clients such as the popular Torrent exchange software may contain essential evidence including illegal images or videos, stolen copyrighted and intellectual property. Information about files being downloaded, shared and uploaded can be a substantial addition to collected evidence base.

Multi-Player Online Games

Conversations occur between and during gaming sessions in many popular multi-player games such as World of Warcraft. Why not extending the evidence base by analyzing chat logs extracted from these games? A confession has already been made in a WoW chat about a murder [5].

Multimedia Content

Still images and video files should be analyzed for their content. Tools such as Belkasoft Evidence Center 2012 can help investigators automate the analysis by detecting things such as pornography, human faces, or scanned images of text documents saved as picture files.

Types of Digital Evidence

In this article, we'll talk strictly about digital evidence available on the PC or, more precisely, on the computer's hard drive and live memory dumps. This leaves the entire domain of mobile forensics aside, for a good reason: mobile forensics has its own techniques, approaches, methods and issues.

Types of digital evidence include all of the following, and more:

- Address books and contact lists
- Audio files and voice recordings
- Backups to various programs, including backups to mobile devices
- Bookmarks and favorites
- Browser history
- Calendars
- Compressed archives (ZIP, RAR, etc.) including encrypted archives
- Configuration and .ini files (may contain account information, last access dates etc.)
- Cookies
- Databases
- Documents
- Email messages, attachments and email databases
- Events
- Hidden and system files
- Log files
- Organizer items
- Page files, hibernation files and printer spooler files
- Pictures, images, digital photos
- Videos
- Virtual machines
- System files
- Temporary files

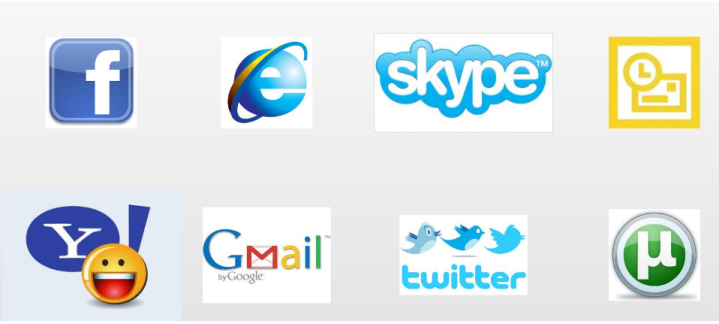

Figure 2: a typical set of communication products

Retrieving Logs and History Files

Logs and history files contain a great deal of essential evidence. Chat communications are often accompanied with timestamps and nicknames of the other parties, allowing figuring out exactly who the respondent was. Determining the exact location and name of these files is an essential first step required to perform further analysis.

Recent versions of Windows typically keep user-created and application-generated data in AppData, Program Files, and Documents and Settings folders. In Windows Vista and Windows 7, the AppData folder does not have a fixed location on the disk, which further complicates the search. In addition, these systems maintain a virtualized storage for applications launched with lower than administrative permissions (AppData\Local\VirtualStore). These locations are commonly overlooked by investigators. Even the well-known Documents and Settings can bear different names depending on the default locale of a particular version of Windows. For example, it can be names “Мои документы” or “Dokumente und Einstellungen” instead. Computer users can complicate the analysis even further by moving or renaming common files.

After you’ve found files of interest by analyzing Windows Registry and applications’ configuration files or performing a manual/automated search, you want to extract data out of them. To do so, you have to know the exact format of each of the source files. Today, thousands of different formats exist, calling for technical knowledge of format specifics – or simply for a tool to automate the task. Fortunately, many modern applications utilize well-documented formats that easy to analyze. For example, SQLite databases are used by Skype and ICQ, the popular XML format is utilized by MSN messenger, Mirc chat uses simple text files, and so on.

SQLite databases can be investigated with free SQLite Database Viewer program, while XML files can be easily opened with Internet Explorer.

However, there are many more formats in existence that are way less forensic-friendly. The cryptic, mind-blowing “mork” format utilized by Firefox, or the proprietary PST format by Outlook, or even Blowfish-encrypted OLE-containers used by QQ Messenger are just a few examples. This is exactly the reason why forensic investigators prefer using automated forensic tools instead of manual search and extraction.

Common Obstacles

Computer users have an easy way to make investigations slower and more difficult. The following are just a few techniques used by the criminals to slow down the discovery:

- changing default location of the history files;
- moving or renaming history file or folder;
- hiding and/or protecting history files with file system attributes and permissions;
- deleting history files;
- formatting the entire hard drive in an attempt to destroy evidence;
- encrypt the entire volume;
- not keeping history by disabling all logging (if supported by application).

The majority of computer users are not IT security specialists, so most of these obstacles are no more than simple annoyances that can be overcome easily by spending little effort. Even whole drive encryption, when implemented by an ordinary user, can usually be dealt with.

The following chapters will discuss these techniques in detail, recommending ways to overcome each of the obstacles, whenever possible.

Obscuring Information and Why It Works

The most obvious way to hide information on a disk is giving a file of interest an obscure name or saving it into an unusual location. This trick is so obvious and provides so little protection that no reasonable security policy would ever let it pass; but why is it still being used by the criminals, and, most importantly, why does it still work?

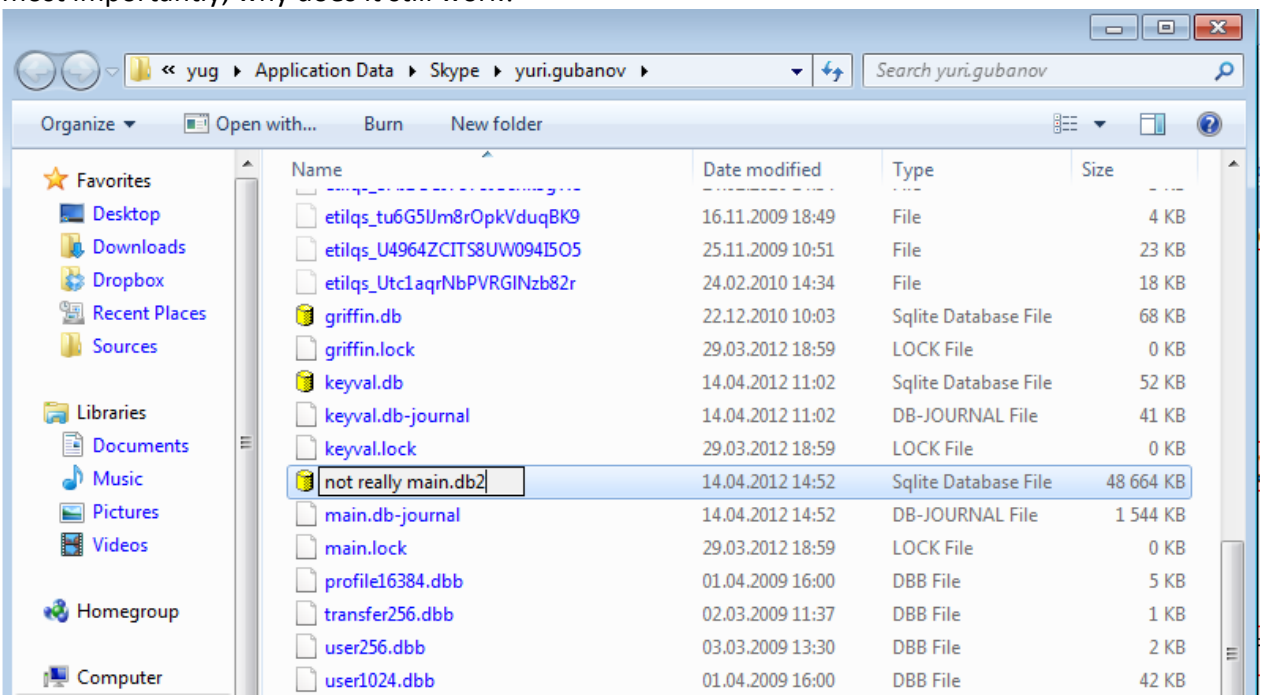

Figure 3: renamed Skype history file

The answer is painfully simple: investigators are time-constrained up to the point they're clogged with mobile phones, laptops and seized hard drives to be analyzed. They often have twenty minutes to a few hours, max, in order to extract all possible evidence. To make things even more complicated, investigators are bound by strict rules. By breaking any one of the rules, investigators may invalidate all extracted evidence.

Retrieving Obscured Files: When File Location Is Changed

One should not expect finding all user information sitting in the default folder, or being located in whatever the default location is for a given type of file (e.g. Application Data or similar folder). Searching the entire hard disk is required in order to locate all unencrypted log and history files. This may produce a certain number of false positives (e.g. not every XML file is an MSN history file), so additional checks are often required (e.g. checking the existence of MessageLog.xsl next to an XML file).

In reality, locating any one of the files is an obvious exercise. As applications such as instant messengers or email clients have to have access to their working files, they store files' locations somewhere in Windows registry or in their own configuration files. One sure must know a lot of things about each and every application being analyzed, which includes literally hundreds of messengers, email clients, peer-to-peer applications and browsers.

In time-constrained conditions of a busy working environment an automated solution is the only way to go. With Belkasoft Evidence Center 2012, investigators can simply launch the scan and rely upon it to discover the files even if they're moved to an obscure location.

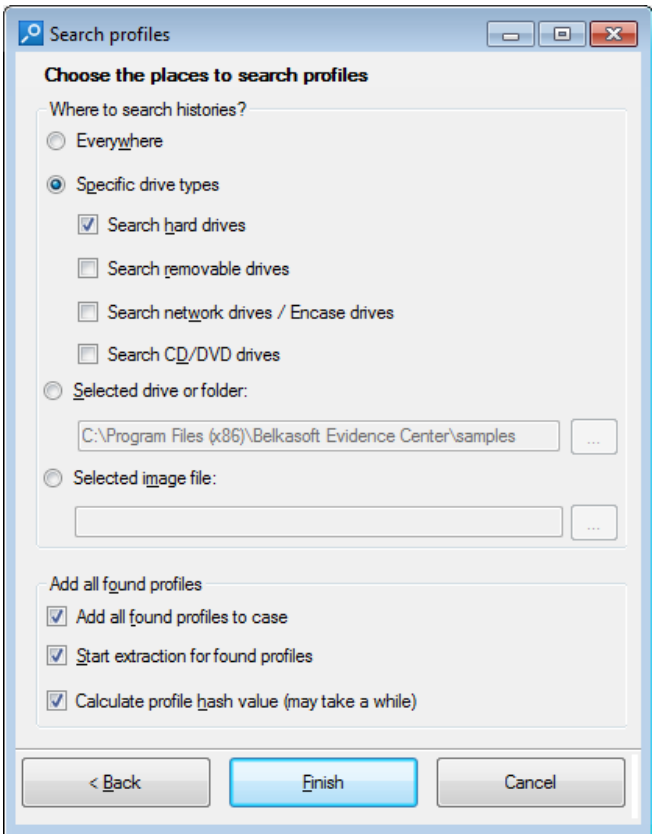

Figure 4: selecting locations to search

Hidden and Inaccessible Files and Folders

Computer users often protect information by assigning file attributes and permissions preventing unauthorized access. Hidden and system files and folders are a common place these days; these will be displayed and even highlighted by every forensic analysis tool in existence. Most forensic analysis tools can bypass security attributes and permission control management (but not encryption) set by the file system such as NTFS access control rights. Special attention should be paid to inaccessible files and folders; otherwise one can miss evidence in folders having access restrictions.

Destroyed Evidence

Attempts to destroy digital evidence are very common. Such attempts can be more or less successful depending on the action taken, time available to destroy evidence, as well as the type of storage device (magnetic hard drive, flash memory card or SSD drive).

The following chapters will discuss common practices and methods used to recover destroyed evidence.

Deleted Files

Important evidence often ends up in the recycle bin. This is especially true for Windows PCs. Literally, deleted files can often be successfully retrieved by analyzing the content of the Recycle Bin, a temporary storage they're placed before being erased.

If deleted files do not show up in the Recycle Bin, there are still good chances to recover them by using one of the many commercial data recovery tools. The principle of deleted file recovery is based on the fact that Windows does not wipe the contents of the file when it's being deleted. Instead, a file system record storing the exact location of that file on the disk is being marked as "deleted". The disk space previously occupied by the file is then advertised as available – but not overwritten with zeroes or other data just yet (however, see the following chapter, "The Issue of SSD Drives"). A good example of such data recovery tools are products developed by DiskInternals (www.diskinternals.com) e.g. DiskInternals Partition Recovery.

By analyzing the file system and/or scanning the entire hard drive looking for characteristic signatures of known file types, one can successfully recover not only files that were deleted by the user, but also discover evidence such as temporary copies of Office documents (including old versions and revisions of such documents), temporary files saved by many applications, renamed files and so on (see "Data Carving").

Information stored in deleted files can be supplemented with data collected from other sources. For example, Skype stores its chat logs in the history database, and keeps internal data that may contain chunks and bits of user conversations in the "chatsync" folder. The format is not officially disclosed, but there are tools available that can analyze such files (e.g. Belkasoft Evidence Center 2012). Thus, if chatsync folder exists, there are definite chances to recover Skype chats even if one have failed to recover a deleted Skype database.

Formatted Hard Drives

Information from hard drives that were formatted by the user may be recoverable with data carving or by using a commercial data recovery tool. However, "may" is the key word here, as the recovery of formatted hard drives is iffy and depends on a wide set of parameters.

Full Format

There are two possible ways to format storage media in Windows: full and quick format. While quick format simply initializes the disk by creating new (empty) file system on the partition being formatted, full format also checks the disk for bad sectors.

From the name of it, one would assume that full format is always destructive – which is not the case. Prior to Windows Vista (that is, in Windows 95/98/ME, NT4/2000 and XP) a full format operation did not zero the disk being initialized. Instead, Windows would simply scan disk surface by reading it sector after sector. Unreliable sectors would be market as "bad".

This behavior changed with the release of Windows Vista. In Vista and Windows 7, a full format operation will actually wipe the disk clean, writing zeroes onto the disk and reading the sectors back to ensure reliability.

Note that SSD drives present a separate issue covered in the following chapter, “The Issue of SSD Drives”.

Quick Format

With the exception of SSD drives, quick format is never destructive. Information from disks cleared with a quick format can be usually recovered by using one of the data recovery tools that support carving.

The Issue of SSD Drives

Above information applies to traditional (magnetic, spinning discs) hard drives and common flash memory such as USB sticks and memory cards. Solid-state drives (SSD) present an entirely new issue.

Solid-state drives represent a new storage technology. They operate much faster compared to traditional hard drives. SSD drives employ a completely different way of storing information internally, which makes it much easier to destroy information and much more difficult to recover it.

The culprit here is the TRIM command. Used to release space advertised as available by the operating system, the TRIM command effectively zeroes information as soon as it’s marked as deleted by the operating system. Write-blocking devices do not help preventing the effect of the TRIM command. An experiment conducted by American researches demonstrated that a TRIM-enabled SSD completely wiped all deleted information in less than 3 minutes. [7] [8] [9]

Traditional forensic methods fail when attempting recovering information deleted from SSD drives, or trying to recover anything from an SSD drive formatted with either Quick or Full format. However, there are exceptions (and exceptions from exceptions).

Information may still be available if the TRIM command was not issued. This can happen if at least one of the many components does not support TRIM. The components include: version of operating system (Windows Vista and Windows 7 support TRIM, while Windows XP and earlier versions typically don’t); communication interface (SATA and eSATA support TRIM, while external enclosures connected via USB, LAN or FireWire don’t); the file system (Windows supports TRIM on NTFS volumes but not on FAT-formatted disks; Linux, on the other hand, supports TRIM on all types of volumes including those formatted with FAT).

Data Carving

Carving stands for bit-precise, sequential examination of the entire content of the hard drive. Carving allows locating various artifacts that would not be available otherwise. The concept of carving is different from the concept of file recovery, even if such recovery is based on signature-search algorithms. With carving, investigators do not rely on files as they may be partially overwritten, fragmented and scattered around the disk. Instead, carving looks for particular

signatures or patterns that may give a clue that some interesting data can be stored in a particular spot on the disk.

Carving is truly indispensable when looking for destroyed evidence. Traditional hard drives may store bits of deleted data (or even entire files) for a long time after the file's been deleted. Sometimes even formatting the disk several times still leaves information that was originally stored on the disk.

Carving Text Data

That said, some binary and most text-only formats can still be carved. Text information is probably the easiest to recover. Blocks containing text data are filled exclusively with numeric values belonging to a shallow range that represents letters, numbers and symbols. When carving for text data, investigators have to take various languages and text encodings into account; Turkish character set differs from Latin, and neither has anything in common with Arabic, Chinese or Korean writing.

There are also multiple ways to represent non-Latin languages. These are called encodings. Different encodings must be taken into account when looking for texts in each supported language. By analyzing information read from the disk in context of a certain language and encoding, one can typically detect text information. In contrast, binary data is pretty much random. It is hence reasonably easy to detect the beginning and end of each text block by counting the number of characters that do not belong to a given language/encoding combination. Once a set threshold is met, the assumption is that the algorithm reached the end of a given text block.

Example of Data Carving

A good example of an application giving excellent results with carving is Skype v.3. Each message stored in its history files is preceded with four bytes ("three double el three"). This signature represents the beginning of each message. Note the important difference between a signature specific to a history file as a whole and a signature specific to an individual message. Once a file signature is lost (such as Miranda history files having a single signature "MIRANDA ICQ DB" at the beginning of the file), it will be very hard to realize that a particular bit stream belongs to a certain history file. However, even if a major part of a Skype history file is overwritten, one can still extract survived messages as each and every individual message has a known permanent pattern.

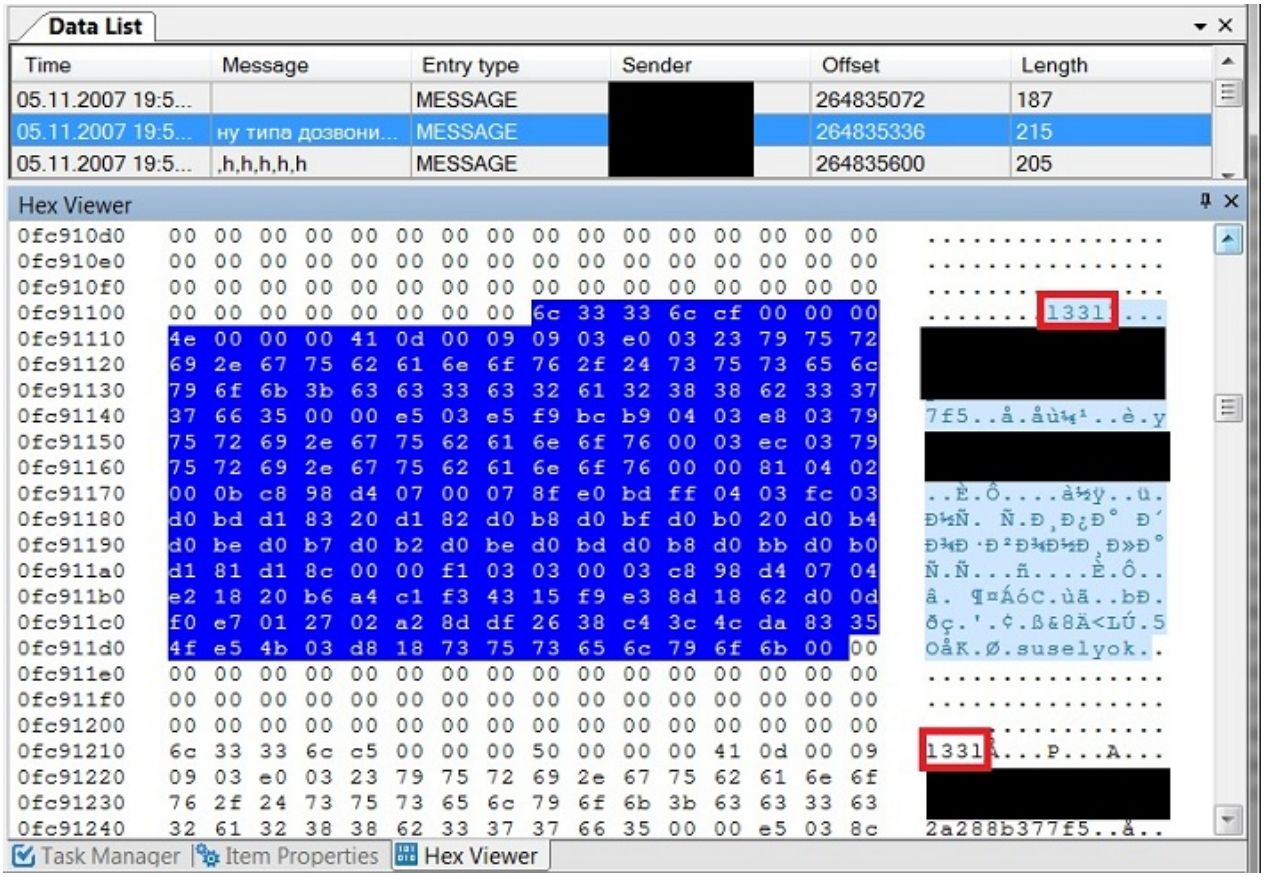

Figure 6: characteristic signature l33l precedes an actual Skype 3 chat message as shown by HexViewer window of Belkasoft Evidence Center 2012

Limitations of Data Carving

Not all data can be carved. Carving is based on characteristic signatures or patterns. For example, JPEG files typically have the "JFIF" signature in the beginning, followed by the file header. PDF files begin with "%PDF", and ZIP archives start with "PK". Some other files can be true binary (without a permanent signature in their header, for instance, QQ messenger or ICQ 98 history files). Text-based files can be an issue because of overwhelming amounts of plain text files that can be stored on the PC.

When Data Carving is Not Available

There are things computer users can do to make data carving impossible. There are numerous applications that can securely wipe information from hard drives. Special algorithms are developed that fill disk space previously occupied by sensitive information with cryptographically strong random data. In "paranoid" mode, sensitive information is overwritten several times to make even clean room type extraction impossible. If one of such applications has been used, data carving is impossible. However, it is possible to detect that a tool like that was used on a disk by performing a statistical analysis of disk data. The white noise contained in the overwritten location is not something that is normally stored on a hard drive, and there are tools that can detect this exact fact. By itself, this can hardly be considered evidence, but the fact can give a warning of unusual activities.

Another way of making carving useless is simply not storing evidence on a hard drive. Although inconvenient through the course of normal activities, this still is a common way to hide browsing or communication histories. If this is the case, only Live RAM analysis may help to recover some recent activities (see "Live RAM Analysis").

Finally, SSD drives can often render data carving useless (see “The Issue of SSD Drives”).

Encrypted Volumes

Disk encryption tools such as BitLocker, PGP and TrueCrypt set industry standard in the area of whole disk encryption. Any of these tools can provide strong, reliable protection, offering a perfect implementation of strong crypto. Normally, an investigator will need to know the original plain-text password protecting the encrypted volume. With many users selecting long, complex passwords, brute-forcing access to one of these volumes is a dead proposition.

However, the very fact that a long, complex password is used presents a way to break into these crypto containers. It’s human nature to keep things easy. Typing a long, complicated passphrase every time the user requires access to a file stored on an encrypted volume is not easy. Most users will opt to typing the password just once after the PC loads. The encrypted container will remain “open” and readily accessible during the entire session. Quite obviously, what’s kept open can be unlocked with an appropriate tool such as the recently released Elcomsoft Forensic Disk Decryptor (www.elcomsoft.com/efdd.html).

The tool works by extracting actual encryption keys (as opposed to user-selected passphrase) from the computer’s memory (Live RAM analysis), Windows page file or hibernation file. A FireWire attack on a running PC can be performed in order to obtain a Live RAM image (see "Live RAM Analysis").

Disabled Local and Remote Logging

While most applications create local history files, some applications (e.g. latest versions of Yahoo Messenger) use cloud storage to keep their log files. Disabling all logging can be an effective technique employed by the criminals to prevent forensic access to digital evidence. When logging is disabled, log files and history files are not being written on the hard disk or stored in the cloud. However, certain logs are still kept in the computer’s memory. Therefore, Live RAM analysis can reveal some or all recent evidence. If the computer is on, a snapshot of its operating memory (RAM) can be taken for Live RAM analysis. If the computer is off, investigators can still analyze swap (paging) and hibernation files.

Live RAM Analysis

Additional digital evidence can be extracted by analyzing the content of computer’s RAM, the PC’s volatile operating memory. Generally speaking, the PC should be powered on in order to perform Live RAM analysis. This is exactly the reason investigators are instructed to leave suspects’ computers on if they are running, and leave them off if they’re shut down.

There are multiple forensic tools available that can save a snapshot of computer’s memory into a file, e.g. FTK Imager (http://accessdata.com/support/adownloads). That snapshot can be then investigated on another PC with various forensic tools including Belkasoft Evidence Center 2012.

Locked Computers

If suspect's PC is locked, investigators should not attempt rebooting the PC. Windows PCs with a FireWire port, used or not, are susceptible to a FireWire attack, unless FireWire drivers are deliberately disabled by the user. Even if a FireWire port is not available, a hot-pluggable FireWire adapter may be used. The FireWire attack method is based on a known security issue that impacts FireWire / i.LINK / IEEE 1394 links [6]. An investigator can take direct control of the computer's operating memory (RAM) by connecting to a PC with a FireWire cable and launching a small application on investigator's PC. After that, capturing the complete memory snapshot only takes a few minutes. The attack exploits the fact that FireWire uses direct memory access (DMA) to control memory. As this is DMA, the exploit is going to work regardless of whether the target PC is locked or not. Explicitly disabling FireWire drivers in Windows Device Manager is the only way to protect the PC against this attack. The vulnerability exists for as long as the system is running.

If nothing else helps and one is preparing to shut down the PC anyway, attempting rebooting the PC, entering BIOS Setup and configuring the PC to load from an external media (USB flash drive or CD/DVD) will leave most of the memory untouched. Having booted from an external media, the investigator can use a RAM dumping tool. This approach will fail if BIOS Setup is password-protected, does not allow booting from external media and the password is not known.

Note that it is essential to performed a so-called "soft" reset by using the "Restart computer" button that may be available on the Windows logon screen (unless blocked by the user). A hard reset with the computer's "reset" switch will reset the content of that computer's RAM, making it useless for Live RAM analysis. [3]

Performing Live RAM Analysis

Data carving is used to carry on Live RAM analysis. Carving can help extracting recent messenger conversations, text messages sent and received, and any other temporary information used by applications, such as Facebook, Gmail and World of Warcraft. Of course, as we're speaking of volatile memory, only the most recent information will be accessible. The information obtained this way may be damaged or partially overwritten, but this is still better than nothing.

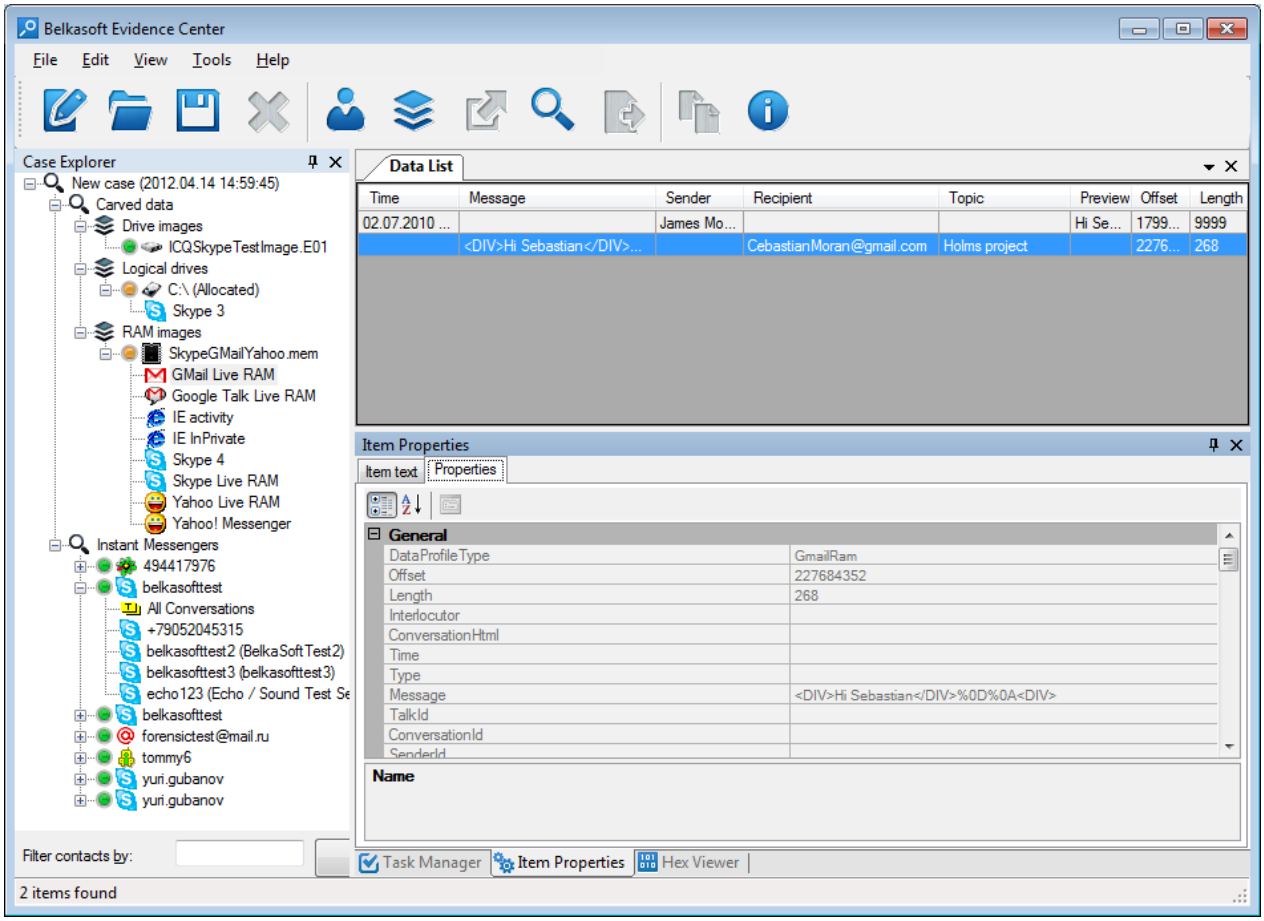

Figure 7: Gmail remnants extracted by Belkasoft Evidence Center 2012 from a RAM memory dump. The messages are already corrupted, and not all fields are available. For example, the first message misses Message and Recipient fields.

Disabling Live RAM Analysis

Disabling Live RAM analysis is possible to a certain degree, but very hard to achieve in practice. Computer users can disable booting from external devices in their BIOS setup; select a strong BIOS password to avoid changing the boot sequence back (can be re-set by investigators quite easily [2]); disable hibernation and virtual memory; block FireWire ports in order to prevent a FireWire attack; lock computer or switch off the computer; set up their system to lock automatically after a certain period of inactivity. While these measures can make Live RAM analysis difficult or impossible, they will lead to significantly reduced performance and are unlikely to be performed altogether as a complex.

Page File and Hibernation File Analysis

There is one important exception when live memory contents may survive shutting down the PC. Windows maintains two types of files to keep snapshots of the computer's memory: page file and hibernation file. These two files may contain live memory artifacts written to a disk as a part of operation system's working routine. The hibernation file is most commonly used on laptops to allow for seamless on/off without losing any opened applications. Page files (there can be more than one) are used on most computers, keeping bits of information from the memory to extent the amount of RAM available to other applications.

These two files can be analyzed using the same carving approach. Windows hibernation files (hiberfil.sys) must be decompressed beforehand as Windows uses compression to reduce file size and improve startup time with less information to be read from the (slow) disk. Belkasoft Evidence Center 2012 can perform this kind of analysis.

Note that the page file and hibernation file get changed or deleted during the system boot sequence. This is one of the reasons investigators are instructed to leave suspects' computers on of they're running, and leave them off if they're not [1].

Real-Time Analysis and Other Considerations

Sometimes, post-factum analysis is not enough. In many cases, IT security and intelligence specialists watch suspected criminals by intercepting their network traffic or logging keypresses and general PC activities with one of the many commercially available keyloggers. These techniques are worth mentioning although, generally speaking, computer surveillance is out of scope of this article.

Worst Case Scenario

Finally, what if the user does everything right to protect their information? If they store everything on an encrypted volume that's configured to dismount when the PC is locked; configure Windows to automatically lock after a period of inactivity; block FireWire drivers to prevent FireWire attacks; set BIOS password and lock boot sequence; disable logs and history files where possible, or wipe them off securely if not; disable paging and hibernation files… if they do all that in a complex, investigators won't be able to extract much, if anything, out of that PC. Investigators can still research victims' computers, analyze Internet provider logs, and collect evidence from the suspect's mobile phones and tablets.

However, most criminals are ordinary people and rather average computer users. More often than not, they believe in security-through-obscurity. They tend to sacrifice security for convenience. They are not normally trained IT security specialists, so they're more than likely to miss out one or more things, opening a way for investigators to break in and collect the required evidence by using methods described in this article.

About Belkasoft

Belkasoft manufactures forensic tools making it easy for an investigator to search, analyze and store digital evidence found in instant messenger logs, internet browser histories, mailboxes of popular email clients, social network remnants, peer-to-peer data, multi-player game chats, pictures and videos.

The company's flagship product, Belkasoft Evidence Center 2012, automatically performs comprehensive analysis of the entire hard drive or its image file looking for many types of supported evidence including live RAM dumps, intercepted network traffic PCAP files, hibernation and page files. More than 110 instant messengers, major Web browsers, all popular email clients, major peer-to-peer (P2P) software, social networks and popular online multi-player games are supported out of the box. In addition, Belkasoft Evidence Center 2012 analyzes still images and video files for pornography, faces and embedded text (locating images of scanned documents).

About the Author

Yuri Gubanov is a renowned computer forensics expert. He is a frequent speaker at industry-known conferences such as EuroForensics, CEIC, China Forensic Conference, FT-Day, ICDDF, TechnoForensics and others. Yuri is the Founder and CEO of Belkasoft. Besides, Yuri is an author of f-interviews.com, a blog where he takes interviews with key persons in digital forensics and security domain.

You can reach Yuri Gubanov at yug@belkasoft.com or add him to your LinkedIn network at http://linkedin.com/in/yurigubanov.

References

[1] Digital Evidence & Computer Forensics, David Nardoni CISSP, EnCE http://www-scf.usc.edu/~uscsec/images/DigitalEvidence&ComputerForensicsversion1.2USC.pdf

[2] How to clear an unknown BIOS or CMOS password: http://www.computerhope.com/issues/ch000235.htm

[3] Understanding hard reset http://h10010.www1.hp.com/ewfrf/wc/document?lc=en&dlc=en&cc=us&docname=c01684768&product=1132551

[4] Google Searches Used in Murder Trial http://ask.slashdot.org/story/05/11/12/167241/google-searches-used-in-murder-trial

[5] Solving a Teen Murder by Following a Trail of Digital Evidence http://www.forbes.com/sites/kashmirhill/2011/11/03/solving-a-teen-murder-by-following-a-trail-of-digital-evidence/

[6] Physical memory attacks via Firewire/DMA - Part 1: Overview and Mitigation (Update)
http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation

[7] TRIM and the Perceived Demise of Digital Forensics
http://www.crowehorwath.com/folio-pdf/BIS12901_ExpertPositioningArticle_lo.pdf

[8] Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Graeme B. Bell Richard Boddington
http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf

[9] SSD firmware destroys digital evidence, researchers find
http://news.techworld.com/security/3263093/ssd-fimware-destroys-digital-evidence-researchers-find/