ESSAYS ON DIGITAL FORENSICS

Introduction

Dear digital forensic reader! (oh yes, cyber incident responder, too!)

In this e-book, Belkasoft has created several articles that delve into various digital forensics topics for your reading pleasure. The variety of topics and our attempt to add a bit of humor to at least some of them, will hopefully help you to read it without yawning, despite the fact that DFIR domain is not the easiest thing on Earth, not even close.

Enjoy the book!

P.S. and yes, eDiscovery specialist, too!

Table of contents

Magic wand or scientific approach? Myths and realities about digital forensic software

There are lots of myths around what can be done with the help of specialized software by analyzing digital media. Some of these myths are derived from movies, others come from general misunderstanding of how software and hardware work. Since general—non-DFIR—investigators can also be considered regular persons, their expectations of what a DFIR examiner can do could be unrealistic.

Here is an example of a request, received by one of Belkasoft customers:

“Can you recover information from this device?”

This may sound funny, but this is the reality of digital forensic experts’ everyday work.

Give us some real magic

> *What types of difficulties can digital forensics deal with? "Give us some examples of what can be perceived as magic"—one of the journalists asked us.*

There are a number of tricks, which do not look magic to DFIR examiners, however some of them look miraculous even to most experienced folks.

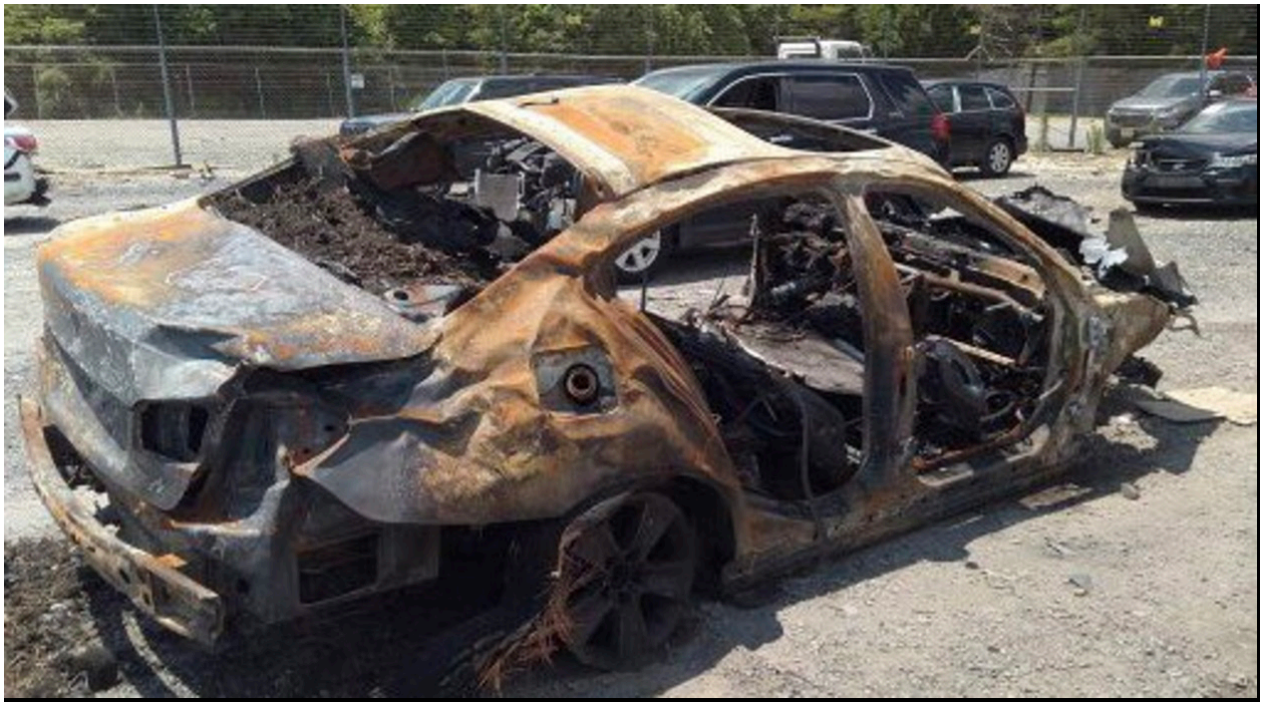
Speaking about the former, it is not a magic to recover deleted or partially damaged data from a hard drive (though it becomes more complicated with the spread of built-in encryption). Corresponding techniques include carving (looking for specific "signature" on a raw data level), recycle bin analysis, parsing of file system snapshots and others. Less common, but it is sometimes possible to recover data deleted on a mobile device. For that, SQLite freelist analysis can be employed; sometimes remnants of user data can be found in various caches on a mobile device.

Though it is commonly believed that special police units can unblock any mobile device, this is not the case for any make and model. This becomes harder and harder for new devices and versions of operating systems. However, for some of them there are some tricks available.

It is also possible to decrypt encrypted data: depending on the encryption method employed, password strength and resources available. Use of specialized hardware (like Passware's Decryptum), rainbow tables and features like "Create keyword dictionary" in Belkasoft X can significantly improve changes to break even strong passwords, which in general case will take a billion years to brute-force.

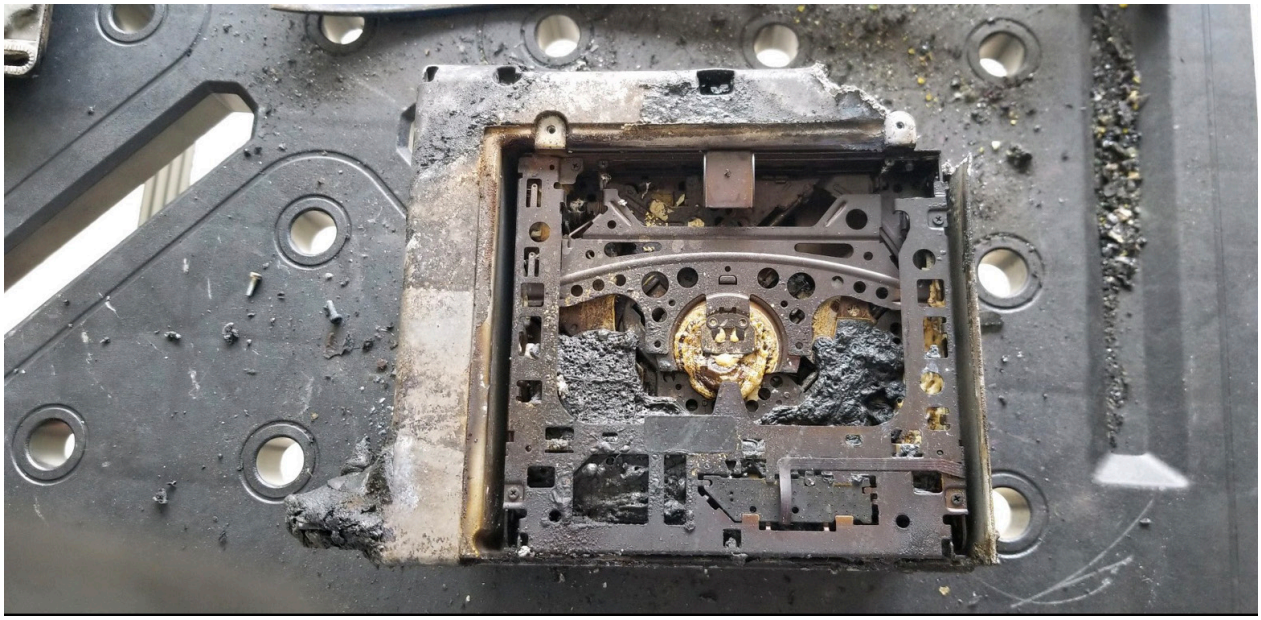
Speaking of cases where only luck helped investigators to recover data, let us mention two cases.

Completely burnt out car



The car does not look good, does it? Being a digital forensics expert, would you promise your fellow investigator that you will recover data from its on-board computer?

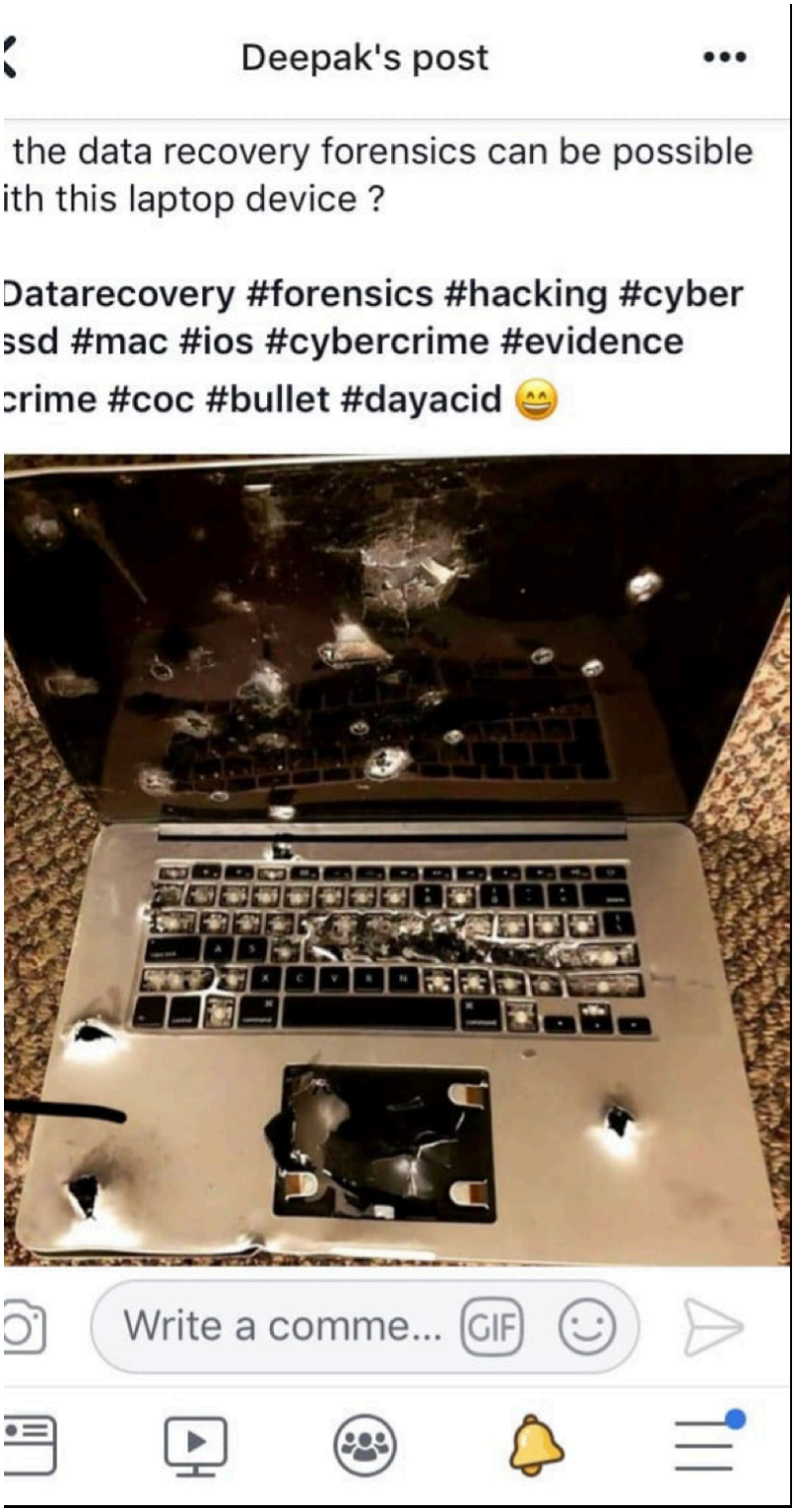
In real life the expert was able to do so. Look at the pictures below for storage devices:



Pure luck, but the drive was readable even though everything else was burnt out. (courtesy of Patrick Eller)

Shot laptop

Another story was told by Deepak Kumar. How big are the chances that this laptop can be analyzed?



Fortunately for an investigator, the hard drive was intact in this case. This still falls under the “miracle” case classification.

Unreal magic

What cannot be done with digital forensics, even with the help of a rare coincidence called “miracle”?

- Data cannot be recovered from ashes like in the very first photo.
- It is n ot possible to get data from a device, if they are never stored on it (though it is a very popular request, like “how do I get all versions of Word document and all editors and their corresponding edits” or “how do I see all occurrences of a USB device plugging into a computer along with all files copied”—though some of this info can be retrieved, there is no full record on both).
- You cannot remotely acquire an arbitrary computer or mobile device.
- You cannot login to an arbitrary computer system in seconds by connecting a magic box to it. Even if such a box exists, most systems will block you from guessing passwords after a few attempts.

You will be shocked, but it is even impossible to read a secret document by enlarging a human’s iris reflection from a surveillance video.

Digital forensic software is not a magic wand, regardless of miracles shown in movies. However, it is capable of doing minor magic (from a regular person point of view). Of course, this magic is not magic at all. Whatever DFIR software can do, is based on scientific approach, mathematics, and meticulous programming.

Browser forensics and the case of casey anthony

> *Belkasoft was extremely lucky to work on this article with Kevin Stenger, a digital forensic examiner who investigated the case of Casey Anthony.*

The case of Casey Anthony occurred back in 2008. Her 2-year-old daughter Caylee was first reported missing, and then half a year later, found dead.

The mother's behavior was suspicious from the very beginning and she was arrested the day after her child was reported missing.

What followed was called "the social media trial of the century" by TIME magazine. The trial did not start for the case until almost two and half years later.

The trial lasted approximately six weeks and there were multiple items of physical evidence, but something was standing apart. It was electronic evidence: some browser searches, in which Casey allegedly made prior to the child's death.

Browser history analysis

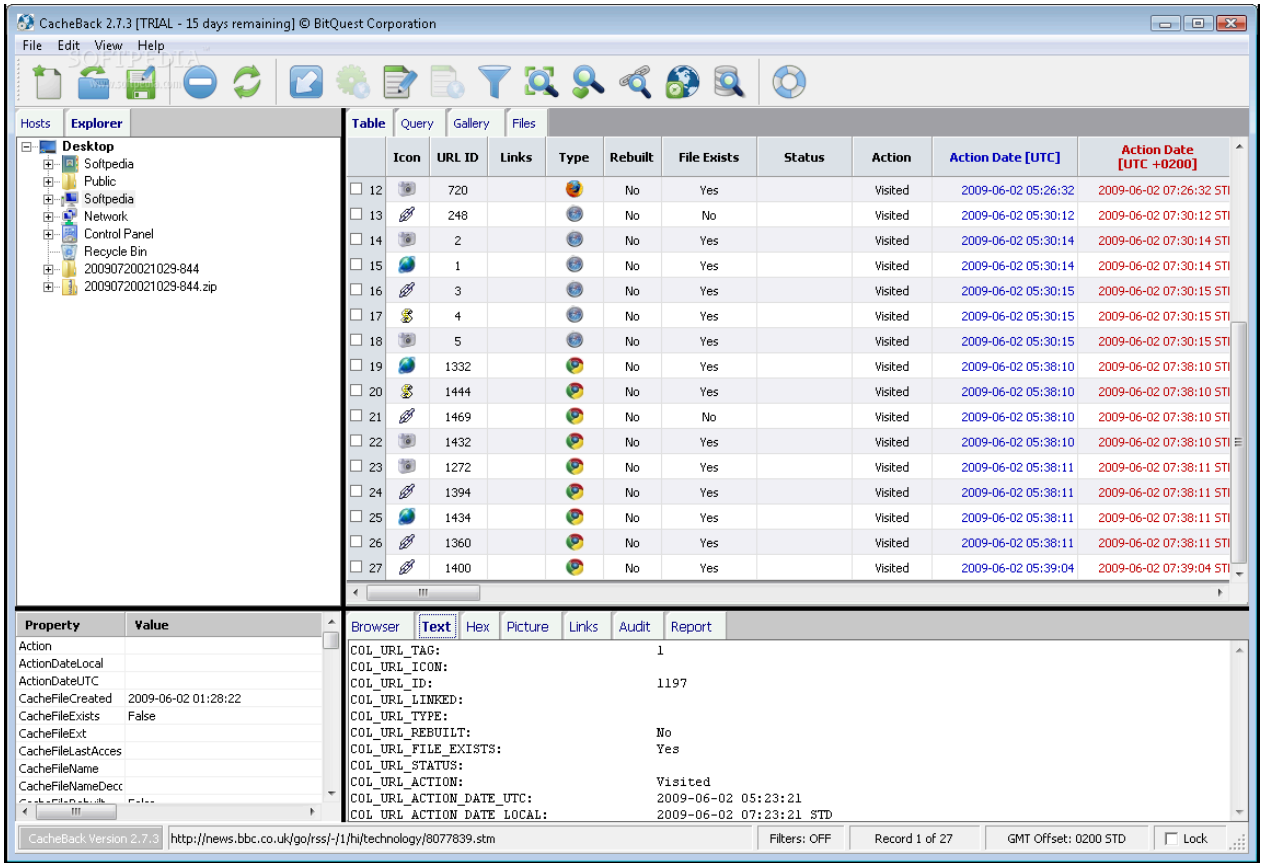
The search terms were quite disturbing and included search terms used in Google for "how to make chloroform" and "neck breaking" among others. The prosecution supposed that Anthony used chloroform to make her daughter unconscious. The software, which was used for the computer analysis, also listed 84 visits to a website which referenced making "chloroform".

> *Though Wikipedia states, with the reference to a TV channel that "police never investigated Firefox browser evidence on Casey's computer", Mr. Stenger witnesses that in fact it did.*

The Firefox history data which this evidence was recovered from was located in unallocated space and could not be attributed to a specific user. The recovered history utilized a Mork database format which had not been used by Firefox for some time. The Mork format is considered to be inefficient and difficult to parse as the database gets larger.

Further complicating the examination of the computer was the fact that all the users in the household appeared to access the computer and user accounts. In addition the CMOS battery had been dead for an extended period of time. Users shutting down the computer and power failures from common Central Florida thunderstorms resulted in the date and time constantly being reset to the default. It also did not appear that the users made an effort to correctly set the date and time after it came back up.

Four separate forensic examination tools were used to try and examine the Firefox artifact. All four produced differing results. Among the software used for the analysis was a tool called “CacheBack”, and its author was an ex-law enforcement officer. CacheBack analyzed Internet Explorer history of the desktop computer, which was seized from Anthony’s home and gave the result described above.



CacheBack user interface

A spreadsheet was generated with the results of the analysis of the Firefox artifact and provided to the Prosecution and Defense. The examiner after consulting with the Prosecution recommended not

presenting the evidence of the 84 visits to the website since the analysis differed between all the applications on this point.It was decided to just present the search terms used in Google which did cross check with the other tools.

Examiners and the Prosecution agreed that the best course of action was to present the digital evidence which could be cross checked and verified and also was corroborated by physical evidence. In this case the air sample taken from the suspects vehicle which had a high concentration of chloroform.

During direct examination by the Prosecution the portion of the spreadsheet containing the Google searches was shown to the jury, judge and attorneys via display. This information was not visible to the visitors or media. The witness was questioned on the information presented. During cross examination by the Defense however the Defense attorney accidently presented to the jury the part of the spreadsheet containing the 84 visits to the website on making chloroform. The Prosecution on redirect then brought to the attention of the jury the 84 visit results that the Defense had accidently entered into evidence. At this point neither the Defense nor the Prosecution was aware that the number of visits to the site was in error.

Was Casey Anthony guilty?

After the conclusion of the case, News Media interviewed several of the jurors. They indicated that they could not come to a conclusion on a guilty verdict. While the digital and physical evidence that was presented suggested a number of different methods of possible homicide no actual cause of death was determined making all of the possibilities just theories without evidence.

The presiding judge was interviewed after his retirement and he concluded that the evidence presented indicated that the suspect had utilized chloroform on the victim but there was no evidence that the death was the result of a deliberate overdose or simple negligence/abuse.

Conclusions

Cross checking results is a vital part of any digital forensics exam. This case presents an interesting problem in what an examiner should do in the event that none of the forensic applications have results that cross-check each other.

Even if you have a preferred digital forensic tool and often rely on it, double check its results by using another digital forensic tool, or manually.

P.S.

Belkasoft is grateful to Mr. Stenger for his comments and contribution to fixing inaccuracies in the original version of this article.

The case of a missing girl and the power of a memory dump

A teenage girl who went missing from her parents' home in the middle of the night. Sounds troublesome, doesn't it?

This story begins on a dark December night, when a 13-year girl slipped out of her door and silently vanished into the darkness after an argument with her parents. For two days the girl was unable to be found. Though the girl's parents reported her missing to the police almost immediately when they found her not in her bed the following morning, the search gave no results. The police checked every location where the girl could naturally hide, including her school, her close friends, and even a dancing club where the teenager was practicing her dance skills and soon ran out of ideas and places to look.

As time worked against the police, the parents started suspecting their daughter may have been kidnapped. The more time that passed, the more worried they became.

Meanwhile, the digital forensics department of the local city police were investigating the girl's personal laptop within their lab. Immediately after waking up the laptop, the investigators captured its memory dump. Computers' volatile memory may contain the most recent evidence such as last-minute chats or messages sent and received with social networks. Upon the analysis, an ICAC task force investigator discovered several recent chat messages from a popular social network.

Checking the girl's social media account was among one of the first things her parents did, with no meaningful results: the most recent chats were not alarming at all. However, the chats found with the help of memory analysis appeared strange to the parents. The chats did not originate from the girl's account. Confusingly, the account that the messages were sent from, appeared to belong to an adult male. Looking further into the account, the girl's parents became even more frightened. The account belonged, if one trusts the profile information, to a 31-year-old adult male.

The next step in the investigation was to attempt to locate a password to that account. Utilizing a known account name, the investigators were able to parse the Chrome password storage, and bingo! They were able to identify a cached password to that very account. The police were then able to successfully log into that account using the newly discovered credentials.

The chat messages inside this particular account shed enough light to explain what had happened. It appeared that the missing teenage girl had created a fake social media account to hide messages from her parents. The girl's parents were able to identify the username of who the messages were being sent to as one of their daughter's friends. As it turned out, the girl had made arrangements to spend a few nights in her friend's home without telling her parents.

A special response unit was dispatched to her classmate's home, where the missing girl was retrieved and safely returned home.

What a happy ending to a seemingly tragic event. An ending that unfortunately does not always transpire in cases like this one. And what's one of the most amazing aspects of this investigation? For two days, the police were attempting to locate the missing girl with traditional methods and failed, while the digital forensic department and their highly technical investigators, who were equipped with proper tools, were able to locate her in less than 30 minutes.

How memory analysis helped to fight against “designer drugs”

This story took place a few years ago. A city drug enforcement unit noticed a rise in the consumption of a few new types of drugs, known as “designer drugs”. Unlike more traditional drugs, these were mostly consumed by teenagers, and consumers were becoming addicted at a frightening speed.

What are “designer drugs”?

These drugs were frequently labeled as “bath salts”, “cactus fertilizers”, “shoe polish”, or even “aquarium fish food”. Designer drugs were specifically designed to circumvent the restrictions imposed by the list of prohibited substances and contain no chemical structures exactly matching those of available (and prohibited) drugs. The slightly altered—compared to already banned substances—formula, allowed them to be semi-legally sold, unless it got banned—and when that happened, a new formula was quickly developed. These drugs were mostly being sold over the Internet from ordinary looking online stores.

In this case, the drugs were sold via street advertising, painted pavements, containing a Skype contact. It was also advertised on a Facebook page. Dealers communicated with their customers via Skype while the Facebook account contained images of the “goods”.

One of the real accounts—now blocked—used to advertise designer drugs on Facebook

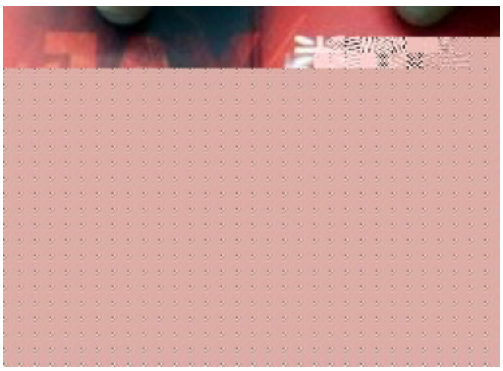
With the amount of contact information available to the police, one of the suspects was quickly identified and arrested, and his computer was seized for an investigation. Apparently, the suspect used elevated security settings, so no immediately visible Skype histories were discovered after a quick manual search.

Facebook communications were cautiously performed with the browser's "InPrivate" mode enabled, which leaves no cached items, no cookies, and no history files on the hard drive. The analysis of the hard drive image returned no data relevant to the investigation, due to the precautions taken by the suspect. The analysis of the page file revealed some traces of information including fragments of chat conversations. However, that was not nearly enough to make the case.

Fortunately, a digital investigator assigned to the case, was able to acquire a memory dump, apart from the image of the hard drive.

> *When given a chance, we always stress the importance of obtaining a memory dump when acquiring a suspect's computer. Memory dumps tend to contain essential volatile evidence, often allowing investigators to establish the necessary links when there is little to no evidence available on the hard drive. To make it easier for investigators to acquire a memory dump, we offer a free Belkasoft Live RAM Capturer tool.*

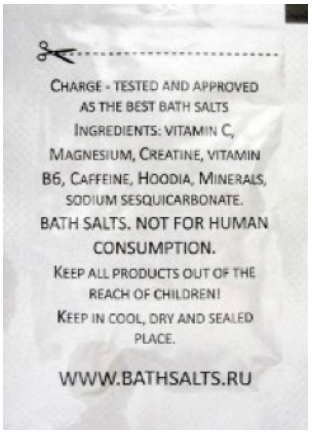
At first, the results were quite discouraging, because pictures of goods, though recognizable, were carved incorrectly:



They were definitely not enough to prove the suspect's involvement in the maintenance of the Facebook page. The reason behind the partially incorrect pictures was memory fragmentation. RAM can be fragmented in the same way that a hard drive can. Simply carving for a JPG or PNG signature will give you the correct beginning of a picture, while some random data may follow, which may belong to another memory process.

Is it possible in such cases to somehow combine pieces together or is it a magic wand expectation?

Belkasoft X (as well as its predecessor Belkasoft Evidence Center, used in that case) has a feature that allows for the extraction of memory processes. If it is switched on during a memory dump analysis, the product will carefully combine fragmented parts of every process into one continuous piece. With this option on, the examiner was able to obtain complete pictures:



Now, when the pictures of these “goods” were recovered, it was important to prove that it was the suspect who uploaded them to the Facebook page, not that he downloaded them from that Facebook page. Fortunately, EXIF metadata was intact within these pictures, while it is known that Facebook strips out most of this information for the sake of security when a picture is uploaded, meaning that such pictures cannot be originated by downloading from Facebook if EXIF data was not removed.

The results of the suspect’s computer analysis enabled the investigator to establish a definite connection between the suspect and the Facebook account used to advertise these designer drugs. In addition, evidence of communication between the suspect and their customers was acquired.

As a result, two designer drug dealers were arrested. The naive label “Not for human consumption”, which you may notice on one of the sachets above, naturally did not help.

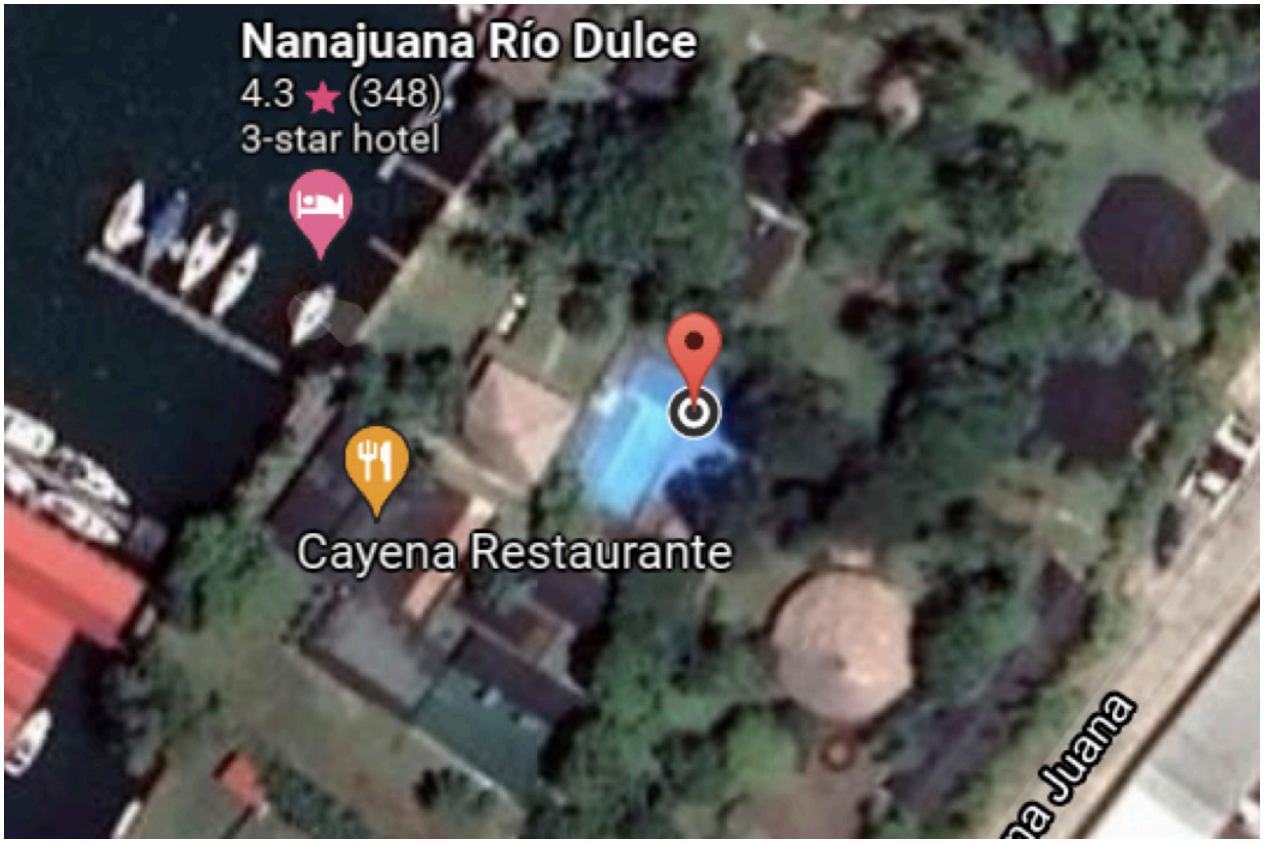
More than 30 kilograms of drugs were seized. Distributed in 1-gram packets, this constituted some 30,000 doses—enough to kill several hundred addicts in one year. Fortunately, this did not happen—thanks to the proper forensic analysis of volatile memory.

Where in the world were john mcafee and an0nymous? A tell-tale sign from exif data

John McAfee was a founder of one of the original antivirus software programs in the world. It has been a decade since the infamous John McAfee was plastering televisions with news of him fleeing the country of Belize. He was named a person of interest in the murder of his neighbor, while living in Ambergris Caye.

McAfee and his neighbor, Gregory Faull, had an on-going feud over McAfee's dogs escaping his yard. A day after their latest disagreement, Faull was found dead from a 9mm gunshot wound and McAfee was nowhere to be found. McAfee fled Belize and headed for Guatemala with his girlfriend and a journalism crew from Vice Magazine. McAfee would remain in hiding for quite some time. While avoiding authorities he turned to taunting the Belize police and the world with social media posts and blogs. He even went so far as to disguise himself as a Guatemalan trinket peddler to evade capture from the police.

All seemed to be going smoothly for McAfee, that is until Vice Magazine posted a picture of McAfee and their editor-in-chief at the time, Rocco Castoro posing together. The picture had been taken with an iPhone 4s at 18:25:26Z on December 3rd, 2012. In addition to the time, we also know the approximate location of where the photo was taken—15 39.49N and 88 59.53W.



But how could someone determine detailed location information along with date and time from a simple picture posted on social media? Behold the power of the Exchangeable Image File Format (EXIF) which is a standard that defines additional information related to an image or other media captured by a digital camera. This additional information is stored in the form of Metadata (i.e. data about data).

EXIF digital image files often use JPEG compression. Below is a listing of some of the common data types can expect to see within image metadata:

- Date and time information
- Camera settings, such as:
  - Camera make and model
  - Rotation
  - Aperture
  - Shutter speed

  - Focal length
  - Metering mode
  - ISO speed
  - and more (depending on the type of camera)
- Thumbnail
- Descriptions
- Copyright Info
- and more

Before diving too much deeper into the story that ultimately led to McAfee taking his own life in a Barcelona prison, let us next explore another example of how EXIF eventually brought down a member of an An0nymous offshoot (CabinCr3w), known as W0rmer.

Higinio O Ochoa III, who holds a Twitter account with the name W0rmer was following the group An0nymous for quite some time and began sympathizing with their beliefs.

Eventually, W0rmer was adopted into An0nOps chat groups, (hacktivists for social justice) which is where we will begin our story.

W0rmer, while sitting in an An0nOps chat, noticed a female come into the chat and begin asking for assistance on a problem that she was seeing with the abuse of dogs. She wanted the group's help to expose the abuse and abusive people. We would later learn that a simple inappropriate joke would ultimately lead to W0rmer's capture, but more on that in a bit.

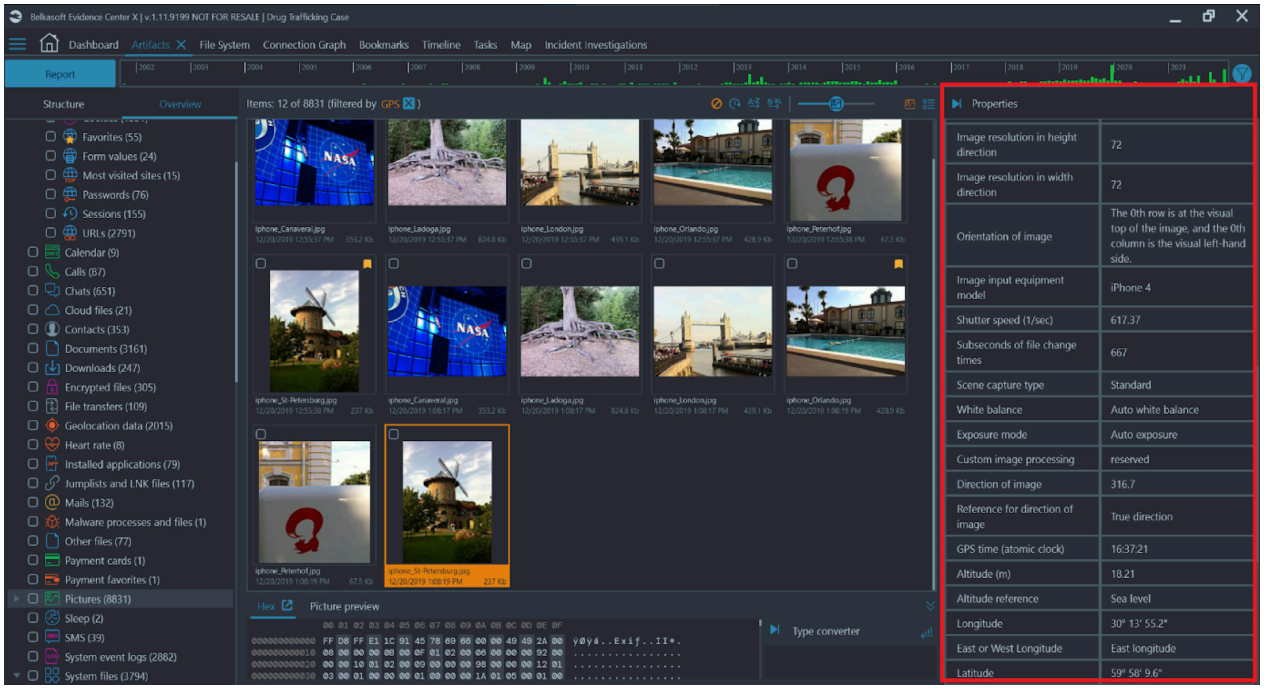
Upon seeing the new female, W0rmer made a crude reference to her breasts saying, «_____ or get the $%&* out. To his surprise, she actually forwarded him pictures of her in a bikini, which W0rmer later adopted and used in his posts to taunt police. W0rmer also fell in love with the girl (eventually marrying her) and noticed that the pictures she was sending contained useful metadata. He could use this metadata to get the location of her house in Australia, which she later confirmed as being accurate. W0rmer of course knew these EXIF photos contained metadata and planned to use them later for his hacktivist activities. He had a method of cleaning the metadata from the photos to make them safe for his use.

W0rmer was executing his plan for social justice by hacking into police department websites within the United States, as he was tired of seeing police officers beating civilians and, in his eyes, abusing their power. He obtained lists of police department websites from other members in the AnonOps chat sites, where he would scan these websites searching for vulnerabilities. When he would find a vulnerability, he would take control of the site and leak database information full of police officer information into Pastebin. When he posted these databases, he would also include pictures of the girl in the bikini holding a sign that said something like «PwND by w0rmer & CabinCr3w. Unfortunately for W0rmer, he accidentally made the mistake of using a non-scrubbed photo that still included metadata, which ultimately led the FBI directly to his girlfriend and eventually straight to w0rmer.

How Belkasoft can help examiners find the smoking gun with EXIF in their cases

Belkasoft X does an outstanding job of scraping EXIF from photographs and presents the data in a very clean and easy to use interface. As an examiner you can even filter only for pictures that contain GPS coordinates. You can also plot these coordinates on a built-in map inside Belkasoft X or even plot coordinates straight to a satellite image within Google Earth.

Additionally, you can export these artifacts into the Keyhole Markup Language (KML) format, an XML notation for expressing geographic annotation and visualization within two-dimensional maps and three-dimensional Earth browsers, developed for use within Google Earth, to display these artifacts in the format designed for the program.



What is shown above, is only a small snippet of the available EXIF data and information about the single photograph that is selected. There are many other great features that Belkasoft offers for the analysis of photographs and other media, such as:

- Face Detection and Facial Groupings
- Skin Detection
- Pornography Detection
- Gun Detection
- Text Detection (OCR in 50+ different languages!)
- Hex Viewer for low-level analysis
- and more!

These chats are not mine! How our test engineer almost went crazy

This is a real-life story that happened to one of Belkasoft's test engineer specialists.

She was partially working from home, and had a Belkasoft product installed on her home computer. At the time, she was carefully testing one of our carving functions. When looking through chats carved by the product, she noticed something strange.

A few of the carved chats looked unfamiliar to her.

This stood out as odd, as the computer belonged to her only, while other family members had their own separate computers and they did not have accounts on hers. This meant that she must have been aware of all chats made from that computer. But she was definitely not recognizing a fair portion of the carved results, and, as she confessed later, was very confused if not frightened.

Before we continue the story, let us explain carving a bit. Carving can be completed from raw data and it disregards files and folders completely. It sees a drive or an image as just one big piece of data where it looks for specific groups of bytes, called “signatures”. An example of well-known signatures may be “MZ” for executable files (though this is a bad signature because it is not quite unique) or “SQLite format 3” for SQLite databases (excellent signature because it is truly unique).

Another thing to mention is the difference between file carving and artifact carving. File carving is when you are trying to recover the entire file and use file signatures (both examples above are signatures of a kind). There are a number of problems that you may encounter with file carving. First is fragmentation: if you are carving a large file as one contiguous chunk following a file signature, it may be recovered partially incorrectly due to the fragmentation (this also happens to memory carving). Secondly, in most cases it is not possible to guess when the file ends. Some formats have a file length in their header, but very few of them do. Besides, you cannot trust this information all the time: if the header is damaged, this may result in an attempt to read, say, a petabyte of data.

The same problem arises when carving utilizes a “header-footer” approach (for files that have footers). A footer is another signature, which designates the end of a file. However, due to the same fragmentation or overwriting issue discussed above, of the tail of a file, a footer may be never met. With what again will result in an attempt to create an enormously large carved file. This is why the length of any carved file in Belkasoft is limited to 5Mb, this helps with saving case storage.

Unlike file carving, artifact carving always results in a small chunk of data. For artifact carving you are looking for a signature and subsequent data for a single item, such as a chat, a browser link, a call, or a similar item, typically measured by a hundred bytes or so.

This is why, while file carving may not recover old deleted files due to fragmentation and overwriting, artifact carving may perfectly recover very old data (of course, of unencrypted media).

This was exactly the case with our test engineer. After taking a deep breath and analyzing the details of these unfamiliar chats (which is possible to do thanks to “Origin path” properties), she was able to understand that it was indeed not her history that she was looking at.

At this point she remembered that she bought the computer second-hand and though it had appeared clean at that time, it was now obvious to her that just a quick format was performed by the previous owner before selling the computer—and as you remember, a quick format does not indeed delete anything (unless this is an SSD drive—but this is another story).

Preserving chain of custody in digital forensics

Introduction

Assuring chain of custody for electronic evidence is more complicated than for other types of evidence, such as a gun, for instance. One of the reasons for that, is that electronic data can be altered without leaving obvious traces. That is why one of the most natural questions which the counterparty may, and will ask in court is: “How can you prove that this evidence (chat/document/photo) has not been altered?” And that is why, apart from well-known actions for preserving chain of custody (like maintaining chain of custody forms), there are additional methods for digital forensics.

This article explains these methods utilizing Belkasoft X, a flagship digital forensics and incident response (DFIR) tool by Belkasoft.

Data collection stage

This is the first stage of every DFIR investigation and is where a chain of custody first appears.

Let us skip the collection of the physical evidence, as we would for non-DFIR items. Digital forensics specifics start at the point of data acquisition. Here, we will focus on what can be done wrong during this stage and what will invalidate the chain of custody.

Working with the original data source instead of a secondary “working” copy of the acquired image will almost inevitably introduce changes to the data. Even if a file’s content is not changed by an investigator, any actions such as file access will change its properties. Though it sounds unlikely for an educated digital forensic investigator, we continue hearing about the use of the original drive, and even the original live system for an investigation. An example of this type of action, could be opening a browser on a running computer of interest and looking through the latest sites visit history.

A slightly better, but still risky approach would be to **work with the original data source that is protected with a software based write blocker**. Software write blockers are notoriously known to not block write attempts due to errors, but this is not the only issue that they may have. The following article outlines an excellent overview of what may go wrong while using a software based write blocker.

If you are using **hardware write blocking devices**, remember that SSD drives cannot be fully protected with such a device. The investigator must be aware of the following potential SSD changes that can irregularly and will inevitably occur, such as TRIM or garbage collection.

The industry standard approach to data acquisition is to create a clone disk or an image of the original device. During the acquisition, the original device must be protected with a hardware write blocker (even though we know that SSD's are not fully protected against data change, this is ultimately the best thing one can do, unless the SSD contents are not encrypted allowing for possible invasive methods of acquisition).

Can anything go wrong and affect the chain of custody even with this approach? Yes! One example would be if one were to clone a hard drive but forgets to sterilize the receiving drive first. If you have not correctly wiped or formatted the drive to work as a clone of the evidence drive, you can get unpleasant surprises originating from older cases, such as artifacts recovered by carving.

To preserve the chain of custody, an examiner must make sure that the data acquired matches the contents of the device being acquired. Possibly the most well-known method for this is hash calculation. It is a good practice to calculate a hash sum for the entire data source and all files inside, before doing any further analysis. Common mistakes during this portion of the investigation could be:

- Not calculating hash values at all. No further comments required.
- Using MD5 only. This algorithm is prone to collisions and, if used, should be complemented by another one, such as SHA1 or SHA256 (Note this link on SHA1 future).

Unfortunately, most of the problem sets discussed above are not feasible for modern devices. You cannot acquire all the contents of a modern

smartphone: there currently is simply no method for this provided by a vendor. Hash calculation is great but it will inevitably give different results for data acquired from a mobile phone, meaning that the two consecutive acquisitions will have different hash values, ensuring nothing.

Generating hash values will also not work for memory dumps. Due to the importance of information (particularly, related to encryption) stored in volatile memory, RAM capturing is a vital stage of data acquisition. However, calculating hash values for a RAM dump makes little sense to prove it matches the original data.

Finally, if for any reason an investigator has to make an image of a running computer or a laptop, hash values will also be naturally different for two consecutive acquisitions.

Having said this, it is still required to calculate hash values to ensure that obtained images and dumps are not amended after the acquisition stage.

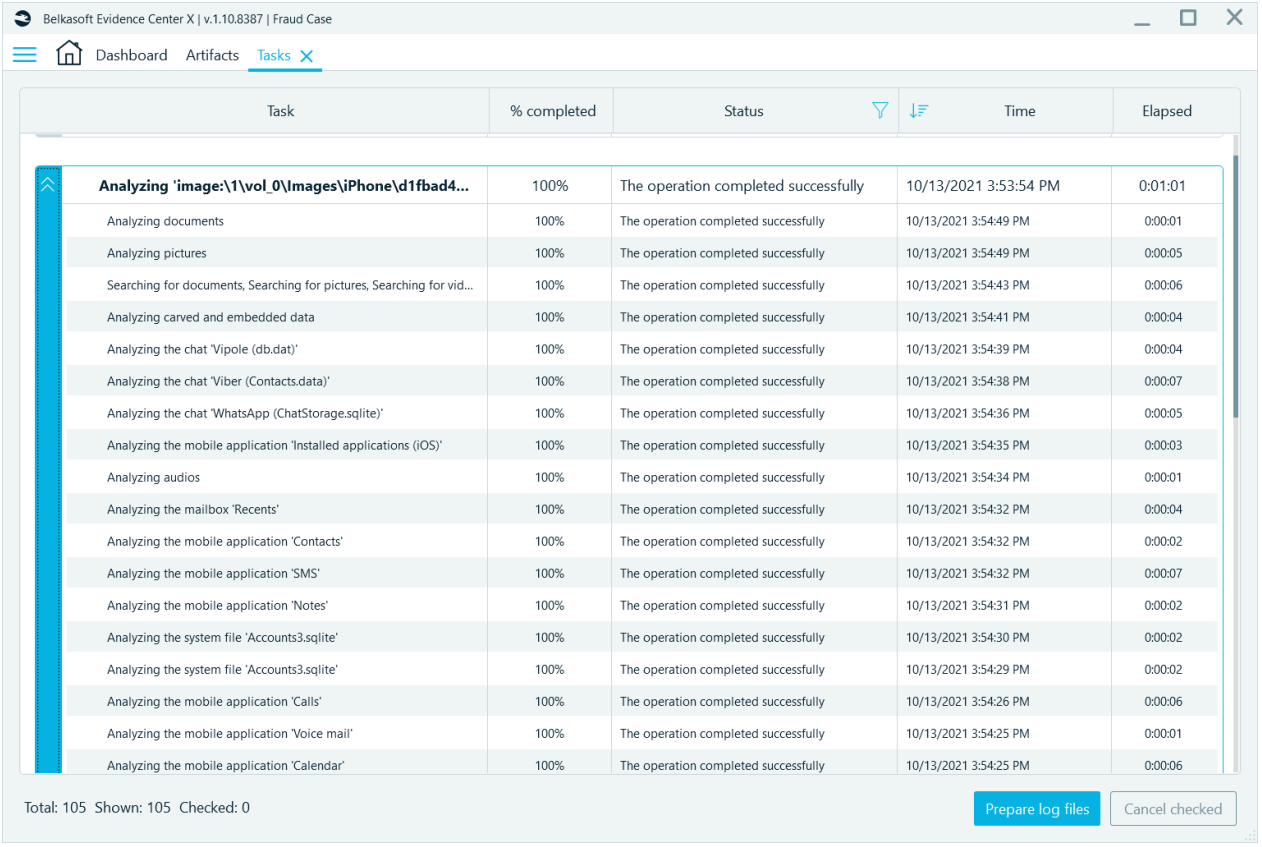
To help assure the chain of custody during the data collection stage, Belkasoft X includes features to forensically acquire hard and removable drives, mobile devices, RAM, and cloud data. The product supports MD5, SHA1, and SHA256 hash calculation for both the images and the files inside.

Examination stage

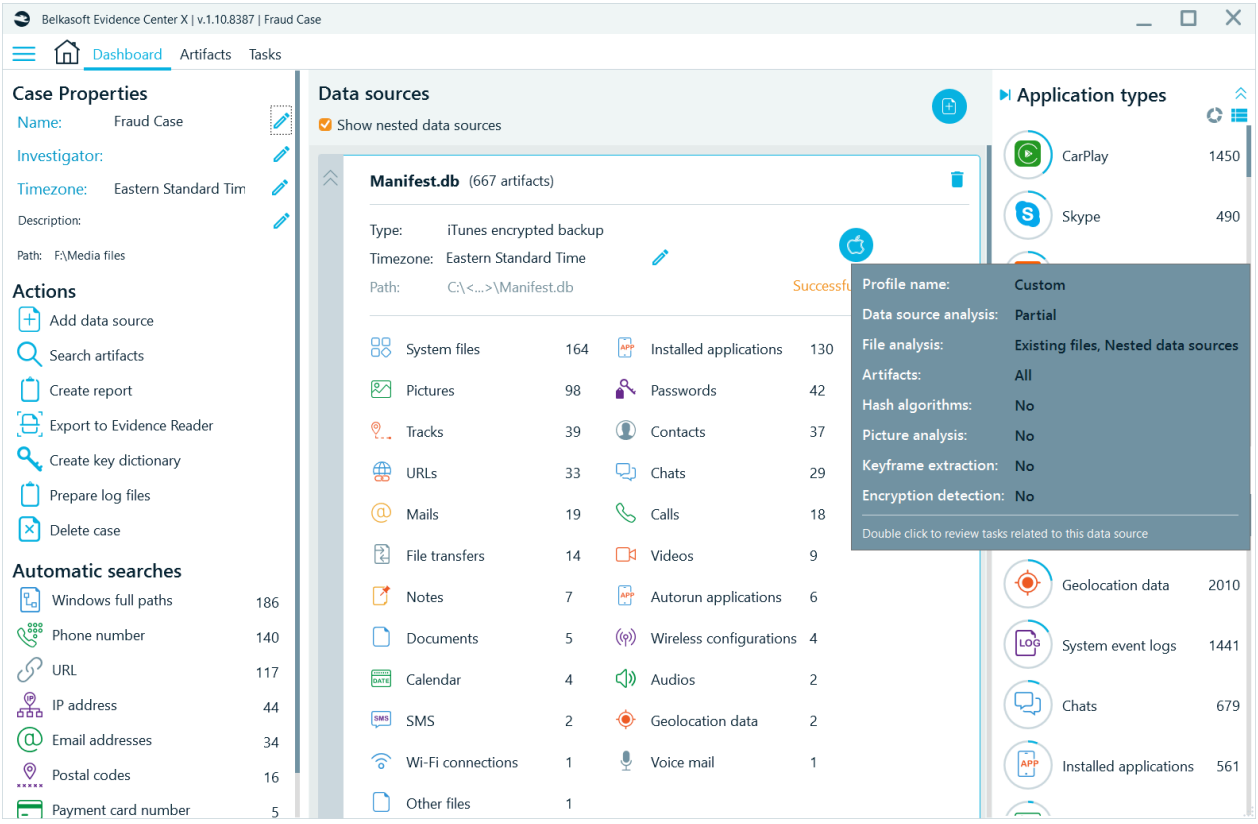
During the examination stage, you must document actions you take within your DFIR tool, to maintain the chain of custody. An examiner must answer the following questions during examination, as the forensic analysis must be repeatable. What was your tool configuration? What types of searches did you schedule? What were the results?

Under this stage, Belkasoft X can help answer these questions, utilizing the following methods:

- Under the Tasks window the product shows an examiner all tasks that have been run for a particular case. These tasks are stored in a centralized database and will be shown even if you re-run the product or re-open the case.



• On the Dashboard, you can review options of analysis that have been run for every data source, by hovering over the data source type icon:



• The product conveniently gives you information such as the case creation date and time, the investigator's name, case notes, and so on.

• For every piece of information, which Belkasoft X recovers out-of-the-box (such as a chat, a browser link, a document, a picture, etc.), the product maintains its Origin path thus helping you to explain where this particular artifact was extracted from.

Analysis stage

There are a number of analytical functions within the Belkasoft X that an examiner can use for the analysis stage, such as photo classification, connection graph visualization, timeline visualization, and more.

There is no specific means included within Belkasoft X for assuring chain of custody for this stage. However, just like within the examination stage, one can see actions that have been run within the product, such as searching for faces within pictures, or hash set match detection, or OCR, in the Tasks window.

The examiner can also include visual information such as a Connection Graph for selected entities and even applied filters, into a forensic report. To do this, one can simply use the built-in reporting function within the Connection Graph window.

Reporting stage

It is important to mention that your DFIR tool report is far from enough to assure a chain of custody. A digital forensic software product includes just a small fraction of what is ultimately needed to ensure a proper chain of custody. An examiner must complement the reporting functions within a product with explanations of what additional tools were used, what the data sources were, how the data was acquired, how the integrity of the data was ensured, and how the data was examined and analyzed. To withstand in a court, your report must clearly describe how the chain of custody was maintained during the entire case.

Since this kind of information is typically out of sight of a DFIR tool, it will not fully provide all the necessary components of chain of custody during this stage. Your organizational templates and best practices will.

All stages

One important issue that needs to be addressed when dealing with the chain of custody, and which relates to all stages, is that an examiner does not only have to maintain the list of everyone who touched the evidence, but they must also ensure that no one else has access to the data. Since electronic evidence exists virtually, there are more ways to occasionally allow such access, than to a physical piece of evidence, such as a gun. For example, leaving a cloned hard drive on a desk in a room, where other investigators work at the same time, breaks a chain of custody. Similarly, leaving one's computer unlocked can potentially invalidate all evidence files stored on that computer.

For a mobile device it is easy to break a chain of custody by leaving just one of the access protocols switched on, including cellular connection, WiFi, or Bluetooth protocols, for a device not protected by a Faraday bag.

Conclusion

Preserving the chain of custody is vital for evidence presented in a court. Not preserving it, or the inability to prove it has been preserved, or even a minor issue with a single step in the chain, may invalidate the examiner's entire evidence collection and possibly deem the examiner's entire investigation inadmissible in court.

When it comes to digital evidence, there are even more mistakes that can take place within this process than with a physical evidence item. The examiner must be aware of these precautions and use best practices described within this, and many other similar articles on the topic. It is advised that the examiner understands their DFIR tool's functionality facilitating the chain of custody maintenance, including forensically sound acquisition methods, their applicability, hash calculation, and more.

Belkasoft X provides you with a number of useful options to prevent issues with chain of custody.

Afterword

After publishing this article, we got a couple of comments, criticizing it for the use of the “chain of custody” term. Our readers argued that what is discussed in the article is related more to the term “evidence integrity” rather than “chain of custody”. While we definitely agree about the evidence integrity being relevant, we found that it may highly depend on a country and its legislation on what is included into the notion of “chain of custody” for digital devices.

Would you like to contribute to the next versions of this article? Please send us your view—what do you think is “chain custody” in your particular country?

Contribute!

How even the best evidence can fail in court

Sometimes even the best evidence can fail in court.

This story is not about digital forensics per se, it is more about the overall process when it comes to working with evidence—including the legal routine that is typically involved. It does not matter whether you performed all the best practices of hard drive or mobile device analysis, if you (or someone who seized the device) failed to perform this step in accordance with local regulations, you run into the potential of the evidence being inadmissible in court.

As an example, there was once a story where police searched the car of a person who they suspected was illegally growing marijuana and they were able to tap the last known GPS location of the suspect. They then drove to that location and found a plantation. However, the court rejected this evidence even though the illegal drugs were found—just because the police did not obtain a proper warrant to use that GPS coordinate. This may sound off, because there was proof of wrongdoing by the suspect, but given that it was found in a non-lawful manner, the entire case was spoiled.

Another story like the one we just discussed was in the press. In this story, a GPS tracking device was put into the suspect's car by police so that they would be able to track the suspect. Again, since there was no warrant for that, the evidence was invalidated. (The story had a continuation, though)

Photo by Wired

> *As it is applied to digital forensics, an investigator or an examiner must not only care about the methods he or she uses for device analysis, but also to ensure lawful seizure of evidence and its proper handling in the lab, including the maintaining of the chain of custody.*

Do you have a story about a great piece of digital evidence, which still failed in the court? Share it with us!

Your experience might help other DFIR experts avoid bloopers.

Share your story

5 Bloopers of a digital forensic investigator

Introduction

Digital forensic investigation is a complicated and challenging job, and it continues to become even more complex due to the rapid development of technology, including pervasive encryption, cloud storage, smartphone security improvements and so on.

It is no surprise that mistakes, which are inevitable with even the simplest routines, happen even in the course of a digital forensic (or an incident response) investigation.

In this article, we will review 5 of the most common mistakes that are often made in the field of DFIR (Digital Forensics and Incident Response).

Mistake #1: Lack of specific training

The size of a digital forensic department in a law enforcement organization or an incident response team in a corporation can vary greatly. Some can have a separate digital forensic lab and assigned digital forensic analysts and investigators, whereas others can consist of several jack of all trade's specialists, executing almost every task assigned.

With that being said, this could mean that digital forensics may be executed by a generalist who may lack specific training, for example, specialized training on a particular mobile acquisition approach.

If you think that experienced investigators and examiners are not "vulnerable" to this mistake, that is not the case. Technology is developing at an unprecedented pace these days, and even the best knowledge of tools and methods are becoming obsolete without supportive regular training. Two years ago, no one knew of the checkm8 vulnerability for iOS devices—now every DFIR specialist must know its specific language and employ this method when they meet relevant devices.

Investigators who care about staying up-to-date, usually utilize several digital forensic tools both open source and commercials. They are constantly reading books, blogs, and forums. They support less experienced colleagues—and can even learn new things by doing this.

Hint: You may also have a look at the list of books, recommended by the Belkasoft team.

Mistake #2: Lack of continuous education

Digital forensics is a very fast and ever-changing field; both investigators and criminals tend to use new technologies. That is why digital forensic practitioners should always be on the cutting edge, keep current with best practices, and be aware of the emerging industry trends. Therefore, as already mentioned in mistake #1, an expert will always need to be learning and self-educating—both on and off the clock.

What happens to those who do not learn every day? Their results become more and more incomplete. They may fail to extract new data, which is extractable with most up-to-date acquisition methods. They may brick a device due to not knowing the latest security measures by specific vendors. As a result, justice may not prevail in these cases.

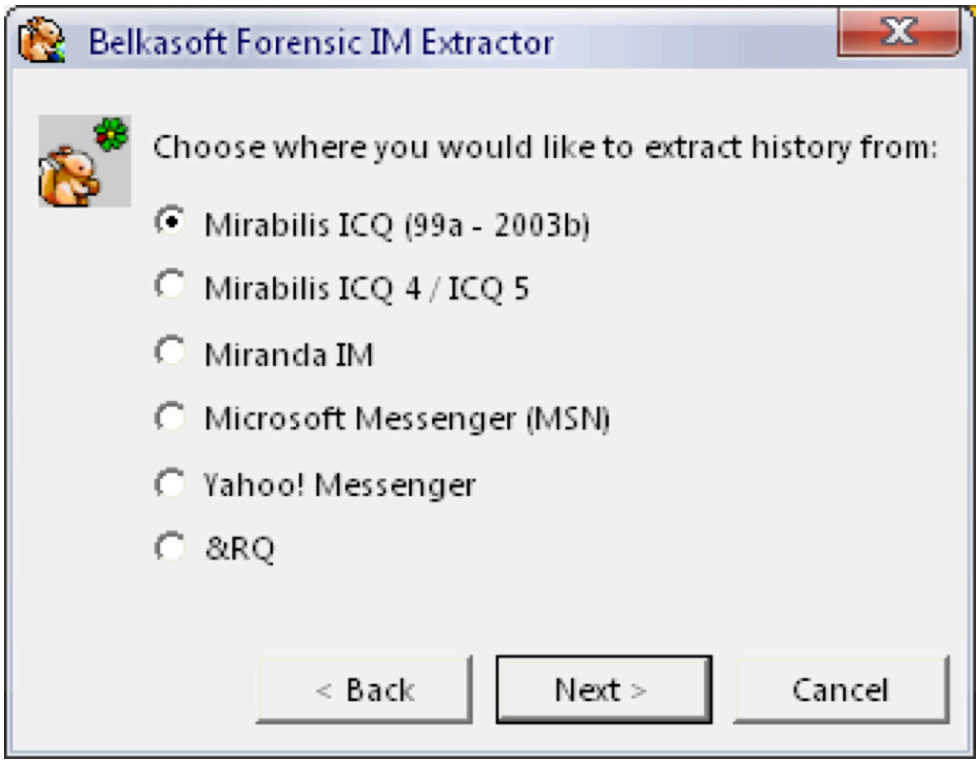
Online and offline communication with fellow DFIR specialists is one of the best ways to always stay up to date. One can mention IACIS and MDFA listservs, various Discord and Telegram channels, Twitter, LinkedIn and Facebook groups—whether vendor-agnostic or vendor-specific.

Mistake #3: Use of “push button forensics” (which is not necessarily a mistake)

The “push button forensics” term was coined more than 10 years ago, and the forensic community considered it to be more as a sarcastic definition of digital forensic tools. In the past, practitioners resisted vendors’ efforts to automate the acquisition and analysis of digital data, as they were sure that automation would make it harder to document, validate, and thus defend their science in a court of law.

Nevertheless, when hard disk drives reached the 1TB range, the Apple’s iPhone emerged and changed the vision of smartphones as a gadget for good, the number of storage media devices increased (phones, gaming devices, external drives, USB sticks, and others), and most of the forensic labs ended up with long backlogs, delaying investigations.

It is no longer feasible to analyze these volumes of data and to be an expert in these unbelievable numbers of popular applications. This is why every DFIR specialist most likely has some kind of automation in their hands now, and the artifact-based approach (by the way, first adopted by Belkasoft around 2007 in our Forensic IM Extractor) is recognized by everyone.



A DFIR tool, which allows an investigator to extract data out of the box without doing a deep dive into bits and bytes of raw data on a data source, can be considered a “push button”. Is it a mistake to use such a tool?

The answer is both “yes” and “no”.

It is hard to define push button forensics as a mistake per se. Most of the digital forensic tools presented nowadays on the market are of that kind. However, there is no tool that can replace the knowledge and skills of its user. Blindly using the results of your tool’s output is definitely a mistake. Knowing a tool’s strengths and weaknesses, comparing the results with similar tools, repeating analysis manually in doubtful situations—is definitely not.

It is worth mentioning that some tools on the market promote using them blindly. Such tools work as a black box and give results without explanations of how they were obtained. No surprise, that conclusions based on such results will not withstand in court, if challenged by a knowledgeable counterparty. A question, which may be asked: “How was this deleted chat restored by Software A?” could appear extremely difficult to answer, if Software A is a black box for you.

A digital forensic investigator must clearly understand that no tool is a silver bullet. Even the best tool can only automate a standard routine, and once your evidence appears not to be falling under “standard” notion, you will have to analyze it manually. Would your forensic tool find an encrypted ZIP file embedded into a PDF document, which was attached to an Outlook email? Would it find deleted SQLite records inside a memory process extracted from a memory dump?

Mistake #4: Failing to assure chain of custody and evidence integrity

Assuring chain of custody as well as integrity for electronic evidence is more complicated than for other types of evidence, such as a gun. One of the reasons for this, is that electronic data can be altered without leaving obvious traces. That is why one of the most natural questions, which the counterparty may, and will, ask in court is: “How can you prove that this evidence (chat/document/photo) is not forged?” This is why, apart from well-known actions for preserving the chain of custody (like maintaining chain of custody forms), there are additional methods for digital forensics.

Possibly the most well-known method is hash calculation. It is good practice to calculate the hash sum for the entire data source and all files inside before doing any further analysis. Common mistakes here could be:

- Not calculating hash values at all. No further comments required.
- Using MD5 only. This algorithm is prone to collisions, and if used, must be complemented by another one, such as SHA-1 or SHA-256
- Working with the original data source instead of a secondary working copy of the image. Though this may work, if you are using hardware blocker devices, remember that SSD drives cannot be protected with such a device. Besides, software write blockers are notoriously known to not block write attempts due to errors. See also this article on many other things, which may go wrong
- Working with a cloned hard drive but forgetting to sterilize the clone. If you have not completely wiped the drive to work as a clone of the evidence drive, you can get unpleasant surprises originated from your older cases

One important factor of the chain of custody is to not only maintain the list of everyone who touched the evidence, but also to make sure that no one else had access. Since the electronic evidence exists virtually, there are more ways to occasionally allow such access, than to a gun. For example, leaving a cloned hard drive on a desk in a room, where other investigators work at the same time, breaks the chain of custody. Similarly, leaving one’s computer unlocked potentially invalidates all evidence files stored on that computer.

Mistake #5: Not cross-checking a DFIR tool results

It can be a habit of the human's brain to keep doing what led to a satisfactory result in the past. In DFIR it may lead to over-using a single tool, which is relied upon too much. If an examiner is used to a particular product, they may use it even for tasks, which are not as well supported by that tool as others.

In reality, there is no single tool, which covers everything in the digital forensics and incident response domain. Even tools, which are great in a particular part of DFIR, may have glitches and issues with a particular file or an image. This is why it is always recommended to cross-check your main tool results, either manually or with a secondary product. This is why a proper toolset for digital forensics must have more than one tool for every particular area of investigation.

Relying too much on a single tool and not cross-checking results may lead to severe issues within a courtroom (read the story above on the case of Casey Anthony), whilst defending results obtained without proper validation.

Conclusion

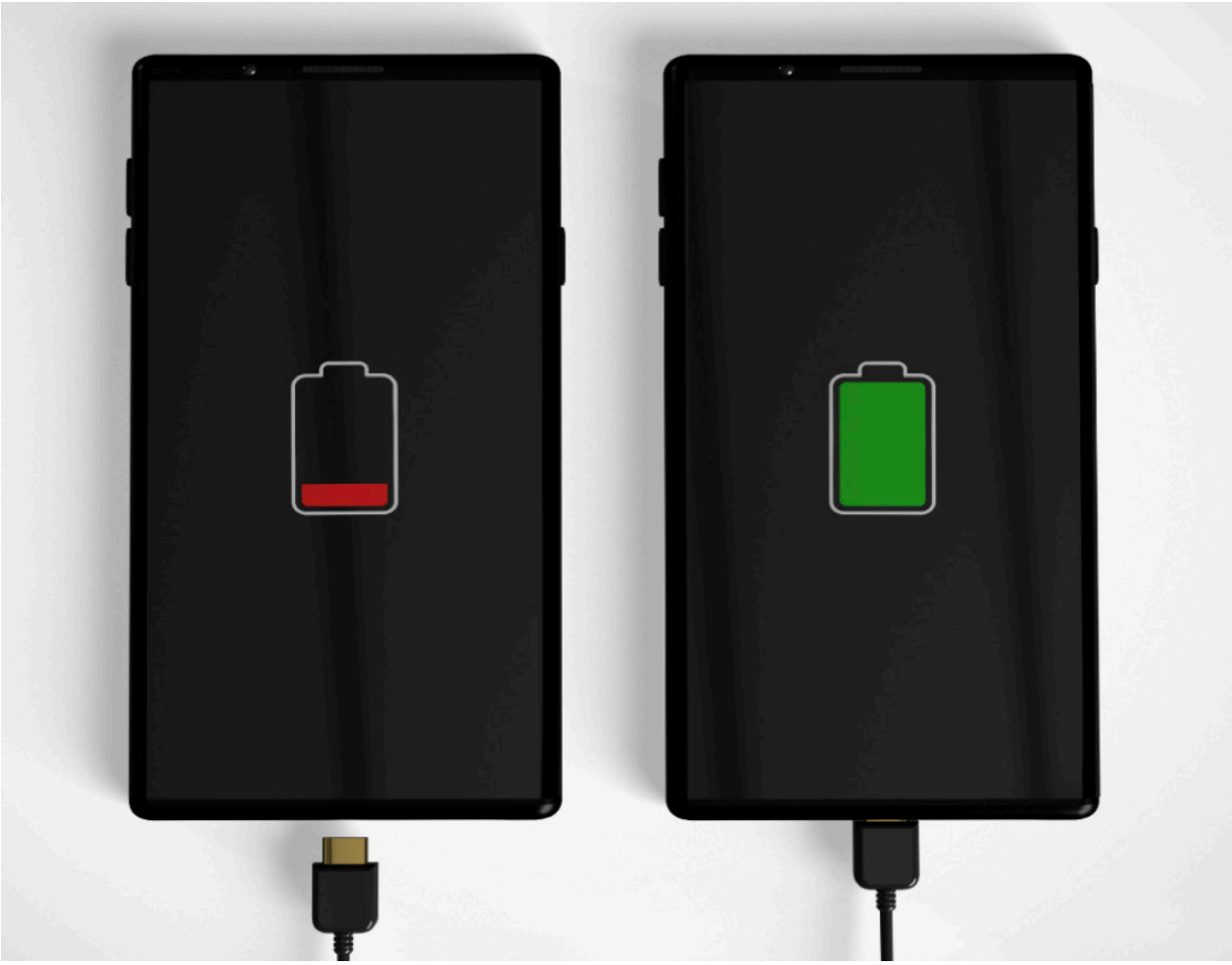
Humans make mistakes. It is not a problem to make a mistake, it is more important how one reacts to their mistake. In the DFIR domain, where every mistake can potentially cause huge and unpleasant consequences, it is especially important to learn from already known mistakes. Learn the field. Do not stop learning even if you think you know everything. Know your tools and be able to repeat their results manually as well as explain how they were obtained. Know how to preserve a chain of custody and specifically which additional methods must be employed for digital evidence.

What other DFIR bloopers would you like us to discuss? Send your ideas and we will be happy to continue this article.

Send your ideas

The importance of fully charged devices in your digital forensic investigation

Investigators and examiners are faced with tough, real-time, on-scene decisions that can have unforeseen consequences weeks or months later. One such decision is how to best handle mobile devices encountered in the field and the different states of these devices. There are many well-known collection tips in the DFIR community such as: if it is off, leave it off, if it is on—capture the screen contents (i.e. any apps that may be running, the battery level, etc.).



Keep confiscated phones in the green

Why might the battery level be important in an investigation? One of the most critical reasons is that if the phone dies you are not just losing power to the device, you are also losing out on a potential opportunity to collect critical volatile data from that current session, the ability to capture device contents when the password is unknown, and much more.

On the flip side, if the phone is on, there is an increased sense of urgency. Device acquisition must be performed soon - before the phone dies or we must connect this device to charge while it is waiting to be shipped to the lab for acquisition and analysis.

When a device is on, we know that we need to isolate the device from the network and reduce the chance of a remote wipe or loss of data. A good precaution against these possibilities is to place the phone in a Faraday bag and isolate the device. Under more dire conditions, a few sheets of tin foil or something similar can also be used to prevent the device from connecting to a network. This is a problem in itself, as annotated in the NIST Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics, “When the phone’s signal is blocked, it will drain the battery rapidly trying to connect to the network. Keeping the mobile device on, but radio isolated, shortens battery life due to increased power consumption as devices unable to connect to a network raise their signal strength to maximum. To conserve power, some mobile devices are normally configured to enter energy savings mode and shut off the display after a short period of inactivity.” (Ayers, Brothers, Jansen, 2014)

To further complicate this all too frequent scenario, most forensic software products require that a device have a certain level of charge in order to acquire a device appropriately. As the phone loses charge and drops below various battery thresholds, service interruptions and acquisition errors are more likely to occur due to insufficient power.

In these tense and time sensitive moments it is important to keep your wits and remember to collect the phone charger that is used with the specific device and use that for your extraction when at all possible. If you can locate the charger, place it in an evidence bag with the phone. This will help immensely with your acquisition later where typically available extraction cables do not work with your specific device.

Does your phone charging station look like this?

References

Ayers, R., Brothers, S., & Jansen, W. (2014, May). Guidelines on mobile device forensics—NIST

5 More bloopers of a digital forensic investigator (part 2)

The article “5 Bloopers of a Digital Forensic Investigator” was a hit and our readers asked for a continuation. Here you go: “5 MORE Bloopers of a Digital Forensic Investigator.”

Mistake #6: Failure to properly acquire RAM and lost encryption keys

Practically every modern digital device uses encryption. Encryption is everywhere. Modern mobile devices have it built-in by default—without a user explicitly choosing to switch it on. Computers, especially laptops can also have encryption enabled out-of-the-box, whether it is file system-based (APFS) or operating system-based (Bitlocker in Windows) encryption.

Because encryption is so pervasive and common it is most definitely a blooper to switch a running computer off to “dead-box acquisition”. This was a general approach to data acquisition back in the “good old days” before the encryption era. If you power down a modern encrypted device you will likely lose access to all the information you could have obtained and used to break that encryption.

> *Note: be sure to read the ACPO guidelines or similar documents discussing best practices, guidelines and rules for volatile memory acquisition.*

When decryption is necessary, your best chance against encryption is to obtain a RAM dump from the active device. Data in volatile memory may contain decryption keys that could be the difference between success or failure (although we feel it is important to mention, that there is no guarantee that a RAM dump will produce device decryption keys!).

There are many nuances to an effective memory dump as a first step. This process alone has many pitfalls, one is a very wide-spread (not only all too common but frequently costly) mistake of using a forensic tool with a lot of capabilities and a large memory footprint. An example would be FTK

Imager, an excellent tool for various types of acquisition, but a tool that requires far too much memory to be your tool of choice for RAM dumping. Its size is over 20 megabytes, while there are many other tools on the market that are hundreds of times smaller. Needless to say, the larger your tool of choice, the more user data is overwritten in memory when you run it, because the executable is loaded into memory to run.

> *Note: Here is a link to a free, light-weight RAM capture tool, which is under 100K in size: https://belkasoft.com/ram*

Mistake #7: Performing a live browser session

This mistake sounds impossible, but nevertheless, every year we hear quite a few stories of this actually happening. And, it is a mistake that can happen to even more seasoned investigators, here is how:

- An inexperienced DFIR investigator might be tempted to perform live analysis on the device and try to get information only available from a browser executed by a logged in user. A dead-box image would mean that browser data might become encrypted. It is not a trivial task to decrypt such data (though it is possible, Belkasoft's tool can help)
- This mistake may also be caused by the fact that often the first person who gains access to a digital device, might not be a qualified digital investigator at all. Anyone who is not trained on how to properly seize devices, may have the temptation to quickly and recklessly acquire information from the live device, and cause irreparable harm to the admissibility of data in court later.

Attempting live analysis on a device using the suspect's account will likely cause severe problems in court as chain of custody cannot be assured.

Mistake #8: Attempts at brute-force decryption, which are likely to take over a billion years

Modern encryption has proven to be very robust. If a strong password is used, there are no known options to avoid time-consuming attempts to decrypt a file or a volume. This means that unlike algorithms used in the past, which allowed an examiner to test hundreds if not thousands of passwords per second, modern encryption requires multiple seconds per password attempted!

Running a full brute-force attack (in most cases) is not the smartest thing to do. Even with a high performance system, packed with memory and multiple graphics cards, sequential brute-force attempts can take billions of years to complete!

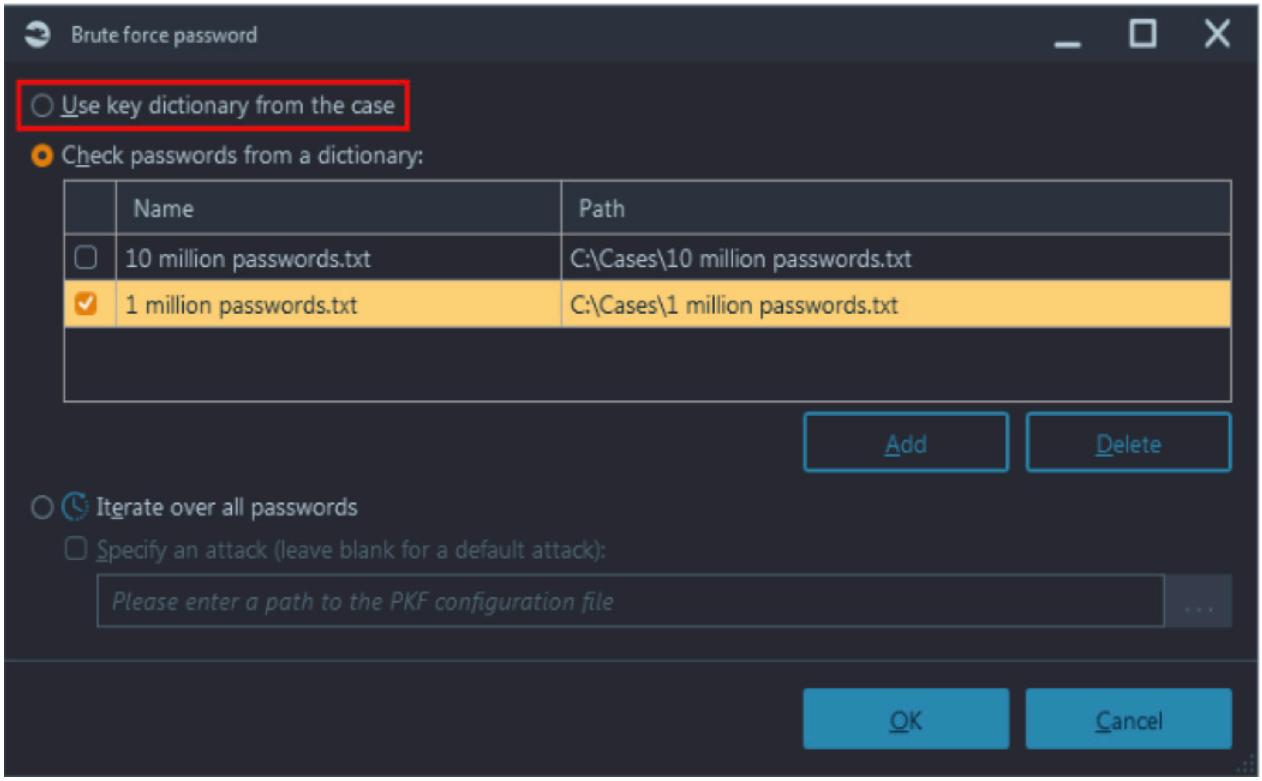
> *Hint: Check out our partner's masterpiece for password cracking: Passware Decryptum*

By sequential brute-force we mean attempts to check passwords in sequential order from lowest to highest (e.g. a, b, c… aa, ab, ac and so on). It is easy to see how checking the vast volume of possible passwords one at a time, and multiplying each attempt by just one second per password, returns a terrifying result.

A better approach would be to try and apply some case-specific knowledge. If you already have some data extracted from a suspect's device (i.e. previously discussed memory dumps or hard drives), that knowledge can be used for decryption. Most people create passwords based on words in their vocabulary, words they use regularly (e.g. their kids names, past car models or cities they lived in). Combining such terms from the case and prioritizing attempts using those potential passwords significantly improve your chances for success.

Since most people reuse their passwords across multiple accounts, it is sometimes enough to find "a weakest link". An investigator may try to crack a password stored in the least secure place first, and then to apply that password to a more strongly encrypted item.

Some tools can help you create a user vocabulary as well. In our product Belkasoft X, this capability is called “Create key dictionary”. This function is available from the product’s Dashboard. Other tools, such as Passware Kit Forensic, can not only attempt to check every term from a key dictionary, but also create so-called mutations and combine different terms into one password. Though the number of mutations and combinations is naturally very large, it is still the best and most efficient approach identified for decryption to date.



Mistake #9: Confusing UTC and local time

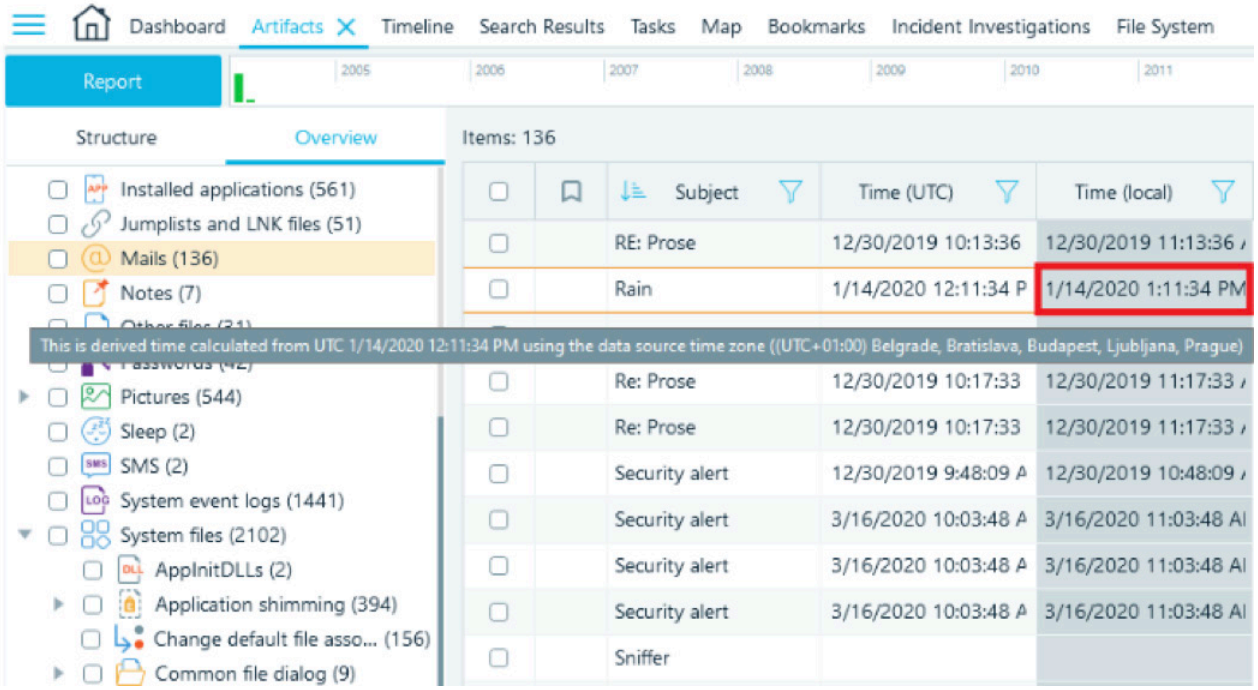
There are many time zones all over the world (technically more than 24). Each and every time zone has its own local time: when it is 12pm in London, it is 7am in New York. Along with timezone conversion, some regions have time adjustments, such as daylight-saving time, when local time is moved one hour later or earlier depending upon the season. The switch to daylight savings is not necessarily synchronized between different countries, which introduces additional difficulties to understanding how time stamps saved in their local time correlate to each other.

The date and time storage standard is Coordinated Universal Time (UTC time). This means most applications and systems are storing timestamps in UTC. However, this may introduce inconveniences and confusion to regular users, who naturally prefer seeing their local time. This is why applications may opt to store timestamps in local time, which is set on each individual user's device.

Now, since the volume of data in today's cases can be overwhelming, it is easy to make the mistake of confusing UTC and local time, stored by different applications. If you do not convert all times to UTC (or local), you may encounter a situation where the order of chat messages are reversed. This occurs if one chat application stores its time in UTC, while the other uses local time.

Your forensic tool may further this confusion for a variety of artifacts if the timestamps are not accurately converted. The issue deepens if you have several data sources from different time zones (e.g. a computer hard drive from Arizona and an iPhone from Washington DC). The forensic tool you choose must allow you to specify different time zones for different devices in your case in order to avoid any timestamp confusion. Not specifying a time zone offset in such a case is another facet to the same mistake.

> *Note: Belkasoft X allows an investigator to set a time zone for the case as well as for every data source. From a column name, you always know whether UTC or local time was used to store a timestamp. The other column, which contains derived time, calculated by the product, will have another background color and a hint, shown when hovering on the column cell. Thanks to automatic time recalculation, Belkasoft X correctly merges different events having different time offsets on its Timeline tab.*



Mistake #10: Bricking a mobile device in evidence

The more mobile devices evolve, the harder it is to capture data from them. Physical images, available when the first smartphone was introduced, are no longer viable due to built-in encryption features. And, standard backups offer a very limited amount of data. This is why most modern approaches to acquire smart device data are based on known vulnerabilities and subsequent exploits.

A common mistake would be to blindly use one of these exploits without first testing it on a donor phone. Any inaccuracy or error in steps (e.g. an incorrect time delay or a slightly different SoC (System on a Chip) model than what is supported by an exploit)—and you can inadvertently brick a device. Losing evidence in this fashion is not just frustrating, it can be ruinous to your case if the device is a critical source of evidence. Best practices involve a careful test run of any acquisition method that utilizes a device exploit by using a similar, or preferably, the exact model device.

It is worth mentioning that sometimes even devices that have the absolute same model and the same SoC inside, may behave differently. Sadly, this means that a successful test-run, even on the same device, is not a 100% guarantee that the exploit is safe for that specific device. However, it obviously increases your chance for success and is better than not testing at all.

As the famous essay from Alexander Pope tells us, “to err is human.” With the proliferation and advancement of technology and the ever increasing complexity of the forensics world at large, this expression has never been more true for the DFIR community. Our hope is that by sharing some of our common mistakes we limit the chance of making a crucial or costly mistake in the future. To advance our field and help new examiners improve we all need to work together and share some of our biggest bloopers, blunders and mistakes. It is important that we all work together and never stop learning from each other.

How even an experienced dfir expert can catch a virus?

The following story was told by our CEO, Yuri. Quoting it first person.

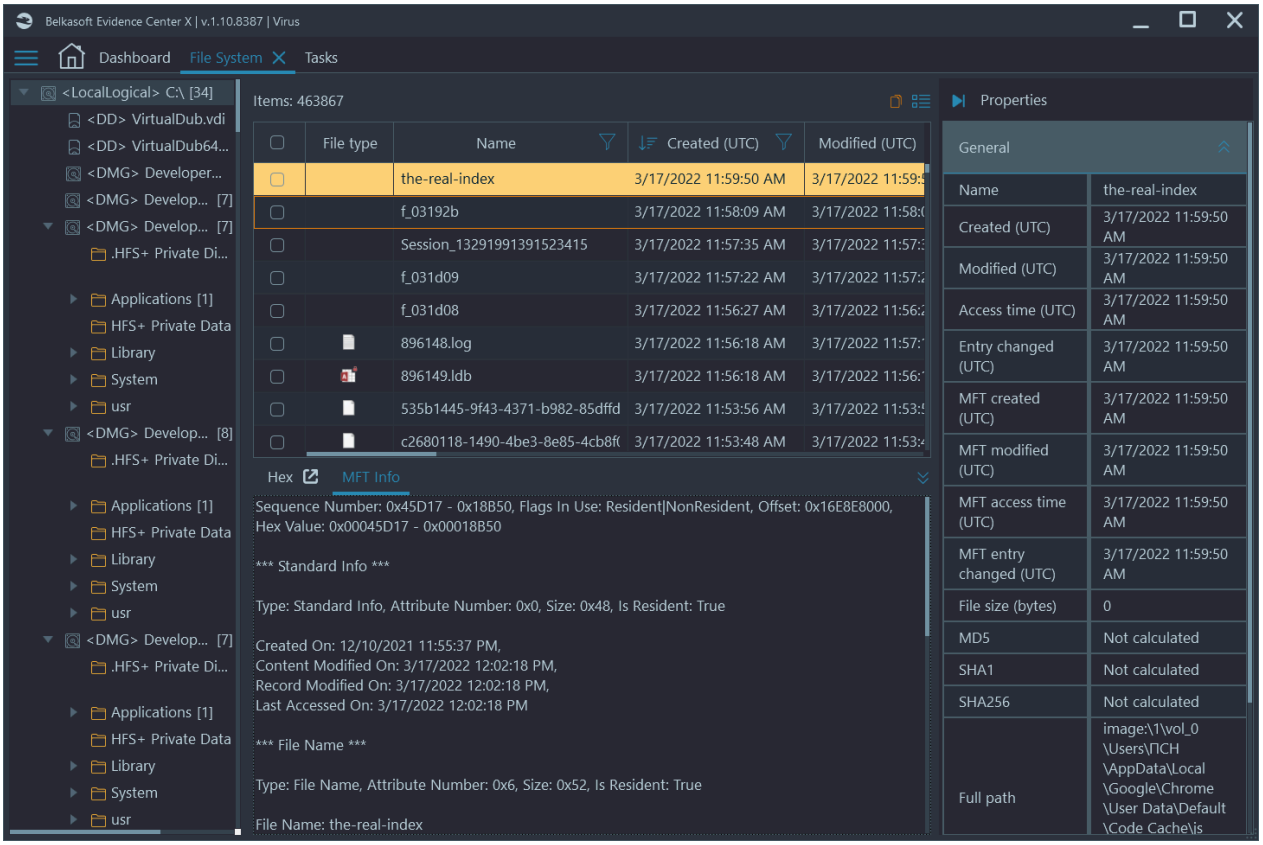
This story took place just a short few months ago. The team and I were chatting with one of our sales employees about a new trouble ticket that had made its way into our management system. We use a service management software which handles our sales and support emails, so every new email creates or updates a ticket.

This ticket in particular was new and what happened next, later **appeared to be a misunderstanding** between our team. From the dialog, I became confident that my colleague had checked the trouble ticket and that the email was legit. For these reasons, I bravely downloaded an attachment from the ticket and opened it on my workstation.

Undoubtedly, **I am extremely suspicious and cautious** when it comes to attachments in both my job and personal communications, even if I receive an attachment from a trusted source. But as I downloaded this attachment, something felt wrong based on the name of the file and accompanying text. I always use online viewers to view the contents of an attachment, rather than offline viewers to open such a file. I always have up-to-date antivirus software running on all of my machines, but of course I do not believe this alone is a panacea.

After opening the Excel document, **I immediately knew something was wrong** from what was displayed within the file and I realized that I am in trouble. I re-read the ticket to make sure that my assumptions were correct and now I clearly understood it was a scam. Cursing myself for stupidity, I instantly disconnected my computer from the Internet and started trying to figure out just how much trouble I was in.

Luckily, I have my tool, Belkasoft X, and the first thing I thought to do was to add my own drive to the product so that I could analyze my own $MFT file. This would help me **understand what new files may have been dropped** by a seemingly weaponized document. By the way, if you are aiming to achieve a similar task, just add your drive into Belkasoft X without analyzing it, go to our File System viewer and simply select a recursive view at the top level of the content pane to be able to sort all files by creation time.



I immediately found the malicious Excel document, selected it, and then sorted all files by creation time. This allowed me to see all files that were created directly after the malicious one was opened. **Surprisingly, I saw only innocent files** including various cache files and system files.

Thankfully, this time **I got off the hook with a slight fright**. When, together with a better specialist in malware than I, we analyzed the file in more detail. The malicious excel document appeared to be targeting a much older version of Excel, and that was why it had failed to drop any additional malicious artifacts and seize my computer. I did, however, go through a few unpleasant minutes though.

There are no conclusions in this story. This is simply a reminder that even the technical savvy can make a mistake, leading to malware installation or really any type of malicious intent.

Even 5 more bloopers of a digital forensic investigator (part 3)

In the previous two articles of this series, “5 Bloopers of a Digital Forensic Investigator” and “5 MORE Bloopers of a Digital Forensic Investigator”, we reviewed some of the most common DFIR mistakes. Both articles have created a lot of good feedback and discussion. In response, we have decided to create one last article and conclude the series with even five MORE mistakes.

You can help improve these articles by sending your ideas of bloopers (and how to avoid or mitigate them) to sales@belkasoft.com.

Mistake #11: Not being ready for a data acquisition or device seizure

The entire DFIR investigation starts with two things: device seizure, followed by the acquisition of data stored on said device. It is a mistake not to know what things may invalidate any collected evidence.

In a perfect world, a DFIR expert would accompany all non-DFIR trained officers to a crime scene. Unfortunately, this just is not realistic as there are not enough good, experienced DFIR specialists available to be on scene every time a crime is committed. This can be a location, timing or resource issue (i.e. not enough DFIR specialists available or free) or sometimes all of the above.

Another example would be a non-DFIR law enforcement (LE) officer leaving the crime scene without recognizing the presence and availability of a viable device for digital evidence collection because they saw “only a TV” or “just a monitor”. As you might have guessed, what they saw as just a TV or monitor could actually be an All-in-One computer, such as an iMac computer. Today, smart devices come in all shapes and sizes, and missing such a device means a lost opportunity for evidence collection.

Another similar blooper is failure to acquire a memory dump from a currently running computer. Pulling the plug on a running device means a

loss of all decryption keys and other volatile data stored in memory (see Mistake #6). This is a very common mistake amongst non-DFIR officers often responsible for device seizure.

In trickier situations, even a DFIR specialist can make this mistake if they are not vigilant and always on the alert. For example, a computer may have self-erasing or even self-exploding data storage, which is triggered by the opening of the system unit cover.

> *Hint: While nothing can replace a digital investigator on-scene, tools like Belkasoft T may facilitate acquiring data even when being operated by a non-expert. Such triage tools are portable and can be run from a special dongle for memory acquisition that is easy to operate and can even store important data on the same dongle for analysis later by a specialist in the lab. These tools help to significantly reduce the error rate with device seizure and data acquisition.*

Mistake #12: Not using write blockers and Faraday bags

This blooper sounds impossible to a digital investigator, but it is still one of the most common mistakes being made today.

Obviously, one has to connect a hard drive to a write blocker before performing any operations, and any mobile devices should be stored in a Faraday bag first. Failure to use a Faraday bag is a severe blooper, and may cause evidence invalidation due to not assuring a proper chain of custody/ evidence integrity, or even troubles introduced by a potential remote data erasure.

There are some more subtle nuances though to be mentioned here:

- A write blocker must be hardware-based. Software-based write blockers are a joke. You simply should not use them (see "Preserving chain of custody in digital forensics")
- Even hardware write blockers will not save your SSD drive from performing its internal erasure routine caused by TRIM and garbage collection. SSD drives are special, see our series of articles on SSD forensics. Written in 2012-2016, these articles are still applicable)

- For mobile phones, the proper routine includes more than just Faraday bags. There are many more things to take into account like keeping the phone charged, keeping (or not keeping) the SIM card inserted, operating in airplane mode, toggling Bluetooth and/or Wifi, not looking into the phone's camera and not touching the fingerprint sensor… and many more do's and don'ts. For more details, we recommend you read: "Practical Mobile Forensics" book.

Mistake #13: Not using available software and hardware effectively

Another frequent mistake is thinking "more is better". Is expensive hardware faster or more efficient than inexpensive hardware? Is software that costs $15,000 three times better than one for $5,000? Would your processing end quicker if you used a 96-core computer rather than a 48-core one?

More is not necessarily better. To give an easy example, many digital forensic software packages rarely involve heavy CPU/GPU utilization (unless performing a password recovery). This means that the CPU is typically not a performance bottleneck and adding more CPU horsepower may only bloat your budget for hardware unnecessarily. What can be a bottleneck is typically your hard drive. Every byte inside an image you are investigating, will be read by your DFIR software. This means the transaction speed of the storage device where the image is hosted has a profound impact on performance and the time required to complete analysis.

This also means that using multiple cores may even… slow things down! If your software reads the hard drive in multiple concurrent sessions, this will make the drive and techniques used by the operating system—like caching—ineffective. As a result, the overall time for the analysis will increase, which is the exact opposite of what you expect!

We once had a case when a customer had a very fancy, shiny 96-core computer, but was complaining about the Belkasoft product performance. After studying his configuration, we gave a recommendation to limit the product to just 48 cores—such an option is available to Belkasoft X users in the product settings. A bit counter-intuitive, but the performance grew

significantly—just because the bottleneck was indeed the hard drive.

On many occasions, effectiveness will also depend on the amount of RAM installed. For Belkasoft X we recommend having 2Gb of RAM for each core used. The product also has a memory limitation setting, which is intended to help customers use the product more effectively, regardless of the hardware configuration in use.

Mistake #14: Not cross-validating results

In the modern world where everyone is in a rush, and when high-tech crime laboratories have tremendous backlogs, this mistake rears its ugly head more often than not. The investigation may consist of ingesting an image into an investigator's favorite tool, browsing through results and generating a report.

Can it work? It can. However, this is not always the case. It is a common point in our industry that no single DFIR software solution is a silver bullet to finding any and all possible evidence. Every software package has strengths and weaknesses and inevitably has flaws. Using multiple DFIR software tools is the best approach to ensuring all possible evidence is found.

What exactly is the cost of an error? See the article "The Case of Casey Anthony" above.

This case is a classic example as to why manual or cross-tool validation is a must, and why trusting results of only a single tool is a blooper.

Here are a few ideas illustrating how Belkasoft can help you validate your results:

- Manual validation. If you would like to check results shown by Belkasoft, we have many tools to facilitate manual validation, such as Origin path property for every artifact, built-in viewers for specific formats such as SQLite, Plist, Registry; and there is a binary Hex Viewer for analysis of raw data behind every artifact
- You can also use Belkasoft X as an excellent secondary tool to cross-check another tool's results. Belkasoft X supports both computer and mobile forensics, and is ideal to complement a variety of other tools.

Mistake #15: Not having Belkasoft in the toolset

As you might have guessed, this chapter is intended to be a little lighter and more tongue-in-cheek to conclude our series.

Despite our walk on the lighter side, we understand that using the right tool is no laughing matter. Given its affordable price and the ability to analyze multiple data sources (including both computer and mobile data sources), as well as the ability to perform memory analysis and cloud forensics, Belkasoft X is excellent as both a primary and cross-check DFIR tool for every digital forensic investigator and incident responder.

A costly sub-type of this blooper is buying separate tools for computer versus mobile phone data acquisition and analysis. You end up paying for two tools when you could have bought just one—Belkasoft X which supports both device types (and many more)—at a lower price!

To avoid these mistakes and many others, here is a secret link where you can learn more on the tool and even download a free trial.

Preventing burnout in digital forensics

The inevitable burnout of a repetitive workflow is not a new concept. People burn out when they do the same thing for too long and they become less interested in both process and result. There is an age-old saying: “Do what you love, and you will never work a day in your life.” Well, this may be the case, but how many of you have started doing more of something that was once a hobby, and then eventually it became work and was no longer enjoyable?

Burnout can come in all shapes and sizes and will probably even look different for everyone, and will likely happen at various stages throughout your career.

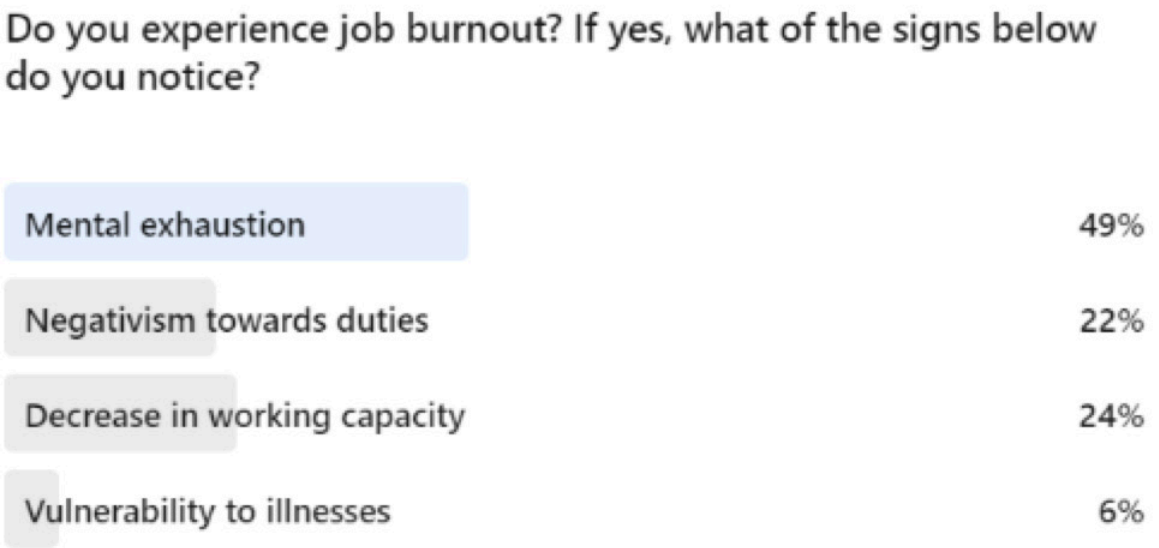
According to the World Health Organization, “Burn-out” is a syndrome conceptualized as resulting from chronic workplace stress that has not been successfully managed.

It is characterized by three dimensions:

- feelings of energy depletion or exhaustion
- increased mental distance from one’s job, or feelings of negativism or cynicism related to one’s job
- and reduced professional efficacy

In DFIR, this burnout is complicated even more by the nature of the work we do. For a digital forensic examiner, it does not matter your sector or discipline, you are likely to be exposed to media files or similar artifacts containing violent or CSAM content. Such repeated exposure introduces a whole new perspective on burnout. We may love every aspect of our job, putting evidence in a report to take down the violent and sick minded individuals who hoard this kind of content. But such exposure can tremendously accelerate burnout.

In the Belkasoft LinkedIn group, we conducted a short survey dedicated to burnout. Here is what some of our readers feel now:



Reduce stressors and limit burnout

- Keep learning: Always challenge your mind and techniques. Try to learn new methods for completing your examination and analysis. A change in workflow might even accelerate old processes
- Your body needs R&R: Do not skip vacations. Even if you feel you do not need a vacation, studies show we do
- According to the Belkasoft DFIR Industry survey 2021, 46% of responders work overtime or beyond the formal time expectation 1-2 or even more times a week. Work from home, remote capabilities, and other benefits of the modern work routine have pros and cons. It is important to delineate as clearly as possible where "work" begins and ends. For example, you can include hours when you are available for urgent communications. If you work in front of a computer the whole day, staring into a computer as a rest will rarely help. Change the type of activity. Sounds insane, but when you feel exhausted, physical activity will actually give you energy. Utilize your unique resources: You have friends, family, associates, connections and social media. Exercise your personal resources for assessment and growth
- Check out the article Somebody Else's Hero: Mental Health In Digital Forensics
- Check out the podcast Mental Stress & Mental Health Awareness in Digital Forensics
- Check our Belkasoft's Jared Luebbert's topic of conversation during a Cyber Social Hub "Hub Cast"
- Talk to an experienced therapist, even if you think you do not need to
- Get up and away from your desk. Going for a walk or getting exercise is a great way to clear your mind
- Check out our latest article on the physical upkeep of your body, and how it can lead to better perspective on work and productivity

There is research in progress on the impact of child abuse investigations and identifying possible protective factors in regard to coping strategies for investigators and personality traits. The study is supported by Newcastle University Psychology Department. You can take part in it and help the digital forensic community.

How Belkasoft helps our users

As mentioned before, examiners are constantly subjected to material that no one should be exposed to. To help our customers have as little exposure as possible, while still effectively performing their duties, we have implemented the following features into our top of the line digital forensic and incident response software:

- Blurring explicit photos detected. Please find more details on this feature in our article “Stay in Good Physical Shape: Look Past the Screen of a Digital Forensic Examiner” below:
    - With the additional ability of unblurring the faces of those in the above-mentioned photos
    - We also offer a blurred content addition to reports, so the disturbing artifacts can be included on reports without exposing everyone
- Allowing hash set analysis to detect CSAM without having to look through photos:
    - With the ability to add or create hash values for this type of indexing and search feature
- By automating the dulland routine tasks Belkasoft empowers examiners to focus on the deeper, more challenging and intellectual work
- Belkasoft also supports the Project VIC hashset search as well as an export format: both 1.3 and 2.0

Conclusion

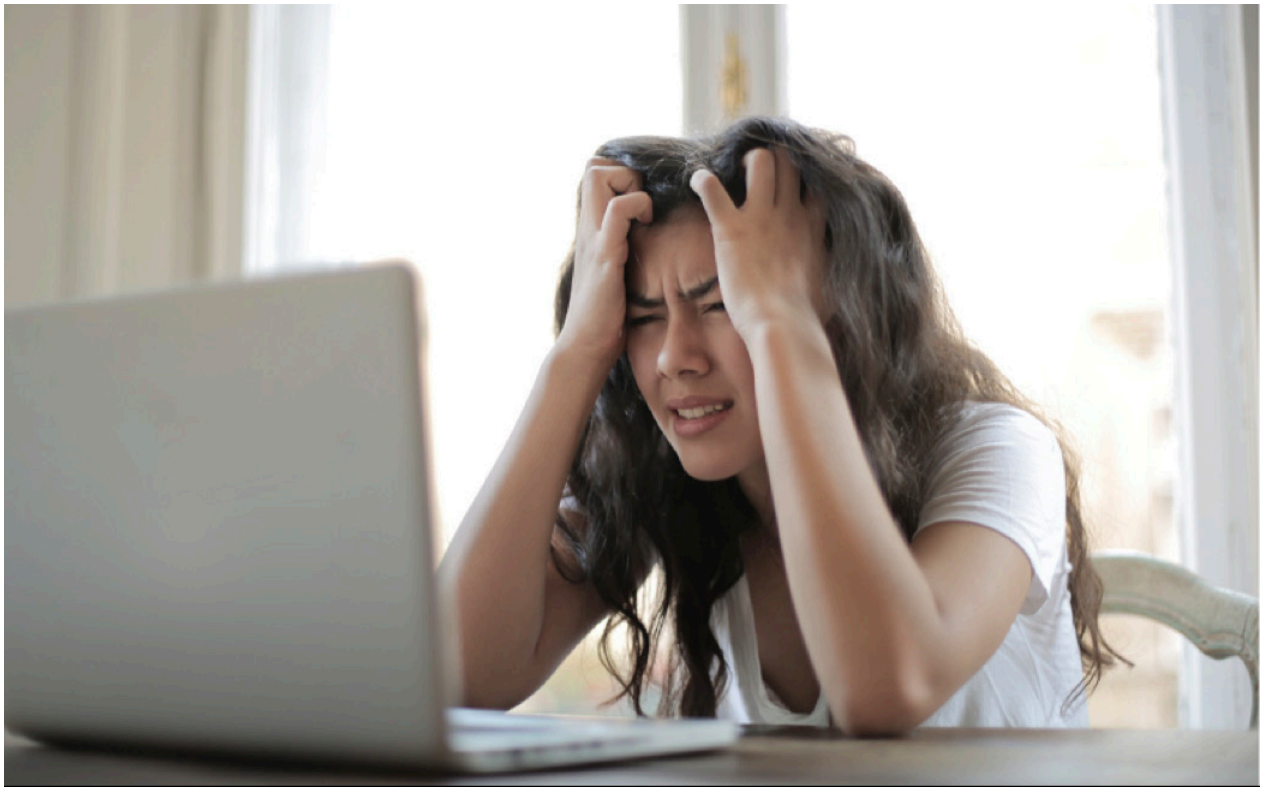
It is inevitable that we will be exposed to material that no one should ever have to see, but the job of a forensic examiner is to uncover necessary and damning evidence that oftentimes will expose criminal behavior. Repeated exposure to disturbing artifacts will most certainly accelerate the process of a burnout, whether personally or professionally. Take the necessary steps to protect your mental state, whether that is taking a long weekend vacation in the midst of a long and gruesome case, or going for a walk to clear your head. We need to protect ourselves, both physically and mentally so that we can keep up the good fight.

The Belkasoft team is always willing to lend an ear to those in need, as well as to continuously improve our digital forensic software to enable good mental and physical health for our customers.

Stay in good physical shape: look past the screen of a digital forensic examiner

As digital forensic examiners, we spend a lot of time sitting at a computer, skipping meals, and often lose sleep to meet project deadlines and in other unfortunate events we lose sleep due to the material that we have to analyze. While doing this, we are also forgetting to take care of ourselves mentally and physically. When it comes down to the wire, self-care and work productivity go hand in hand.

Being productive and alert at work can help you to stay on task, reduce the chance of errors or missing an important artifact, as well as an added bonus of potentially completing your examinations in a timelier manner. Life as a Digital Forensics examiner is more like a marathon than a sprint. Taking a long-term approach, effectively pacing yourself and listening to your body can ensure you are always at your working-best.

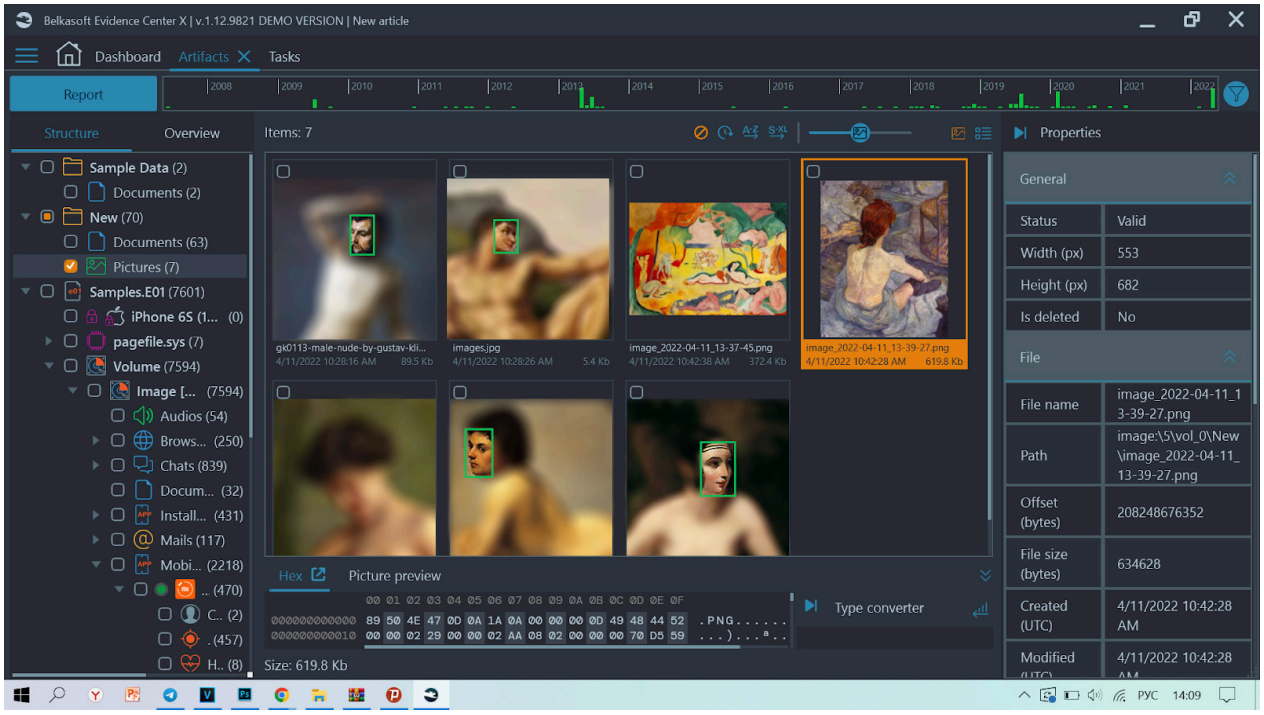


Exercise can provide many more benefits than just weight loss. Did you know that physical activity can help to boost productivity at work through alertness? Whenever you work out, you are increasing the flow of blood to the brain, which in-turn sharpens your awareness of your workflow.

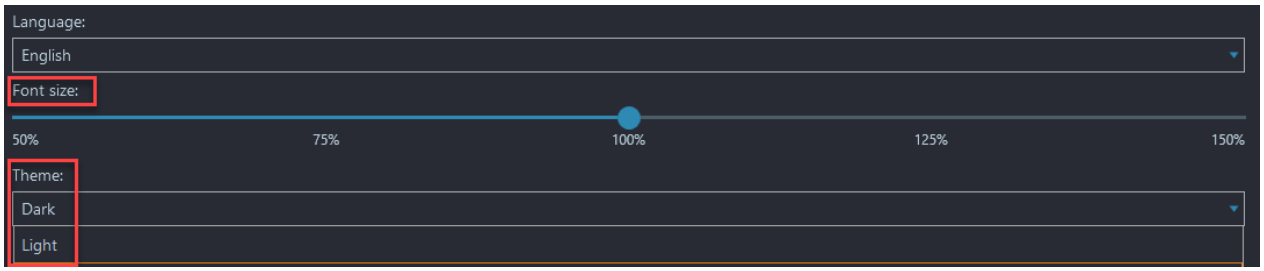
Studies have shown that exercise can improve mental health as well. According to an article by LiveStrong, “Regular exercise can help to curb feelings of anxiety or depression. When you exercise, your brain releases serotonin that helps you feel better and improves your state of mind, making the stresses of work easier to handle.”

Digital forensic examiners and investigators are often exposed to digital material that may be destructive to their mental state, while exercise may not cure this type of exposure, it certainly provides an added benefit and certainly helps the release of potentially repressed feelings of anger or acrimony. Even a ten minute walk a day in between cases or examinations would significantly improve your mental and physical state.

Our Belkasoft X tries to help investigators and limit their exposure to disturbing and graphic content. Belkasoft X can automatically detect images that are disturbing or pornographic in nature with the help of our image analysis features. The examiner also has the option to blur the pictures that are detected as pornography to prevent constant and recurring exposure to disturbing imagery, when it is not required to view. Even better, there is an option that allows for the faces of the individuals in the pictures detected as pornography, to be unblurred so that we can properly identify who is in the picture without the unnecessary exposure of the entire photo.



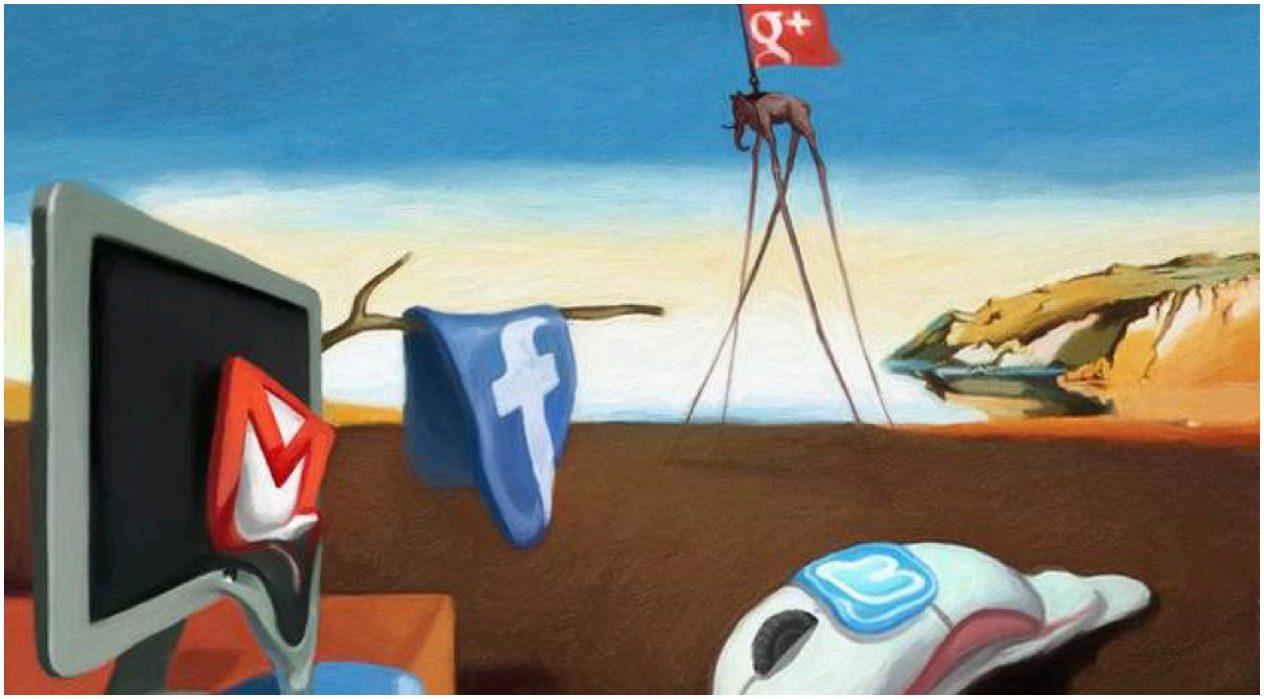
This is just one way that Belkasoft helps guard and protect the mental health of examiners. We also have really great features to assist examiners with their physical health! We help to reduce eye strain through a dark mode capability and varying font sizes to improve readability.



Why ram dumping is so important and how to choose a right tool?

Why RAM dumping?

Volatile memory, or RAM, is used to store data currently used by a running process: whether it is a user application or a system service. This type of memory is much quicker than a regular hard drive but unlike files permanently stored on a drive (unless deleted), data from RAM may disappear instantly. At the same time, it may store data crucial for your case, including passwords in raw format without encryption or encoding, decrypted data otherwise kept encrypted on a drive, decryption keys for various services, apps and WDE, remote sessions data, chats in social networks, malware code, cryptocurrency transactions, various system info such as loaded registry branches, and so on.



This is why it is not argued that capturing RAM contents must be one of the first steps in seizing a running computer or laptop. You can read more on the topic in one of Belkasoft's articles. The article is still quite up-to-date and relevant, with the exception of a freezer attack, which we have not heard about since then and which looks to not be repeatable anymore.

Requirements for a RAM dumping tool

There are a number of requirements for a RAM dumping tool, including the following:

1. Portability
2. Kernel-mode operation
3. Least possible footprint

The last requirement includes obvious items like not writing a dump to a hard drive of a computer that is being captured, leaving as few traces on a host computer registry as possible and not using the Windows' Temp folder. It also implies that the tool executable files and dynamically linked libraries occupy as small of a volume of volatile memory as possible: otherwise the tool is going to overwrite potentially useful data with its own code and thus make a part of the data unavailable.

This is one of the reasons why we regret to see recommendations repeated year after year on the use of tools not specifically designed for RAM capturing. It seems obvious that if a tool has multiple functions, the extra functionality occupies more space than is needed when an executable is loaded into RAM. We strongly believe that a digital forensic investigator or an incident responder must use only tools solely devoted to one single function—capturing RAM.

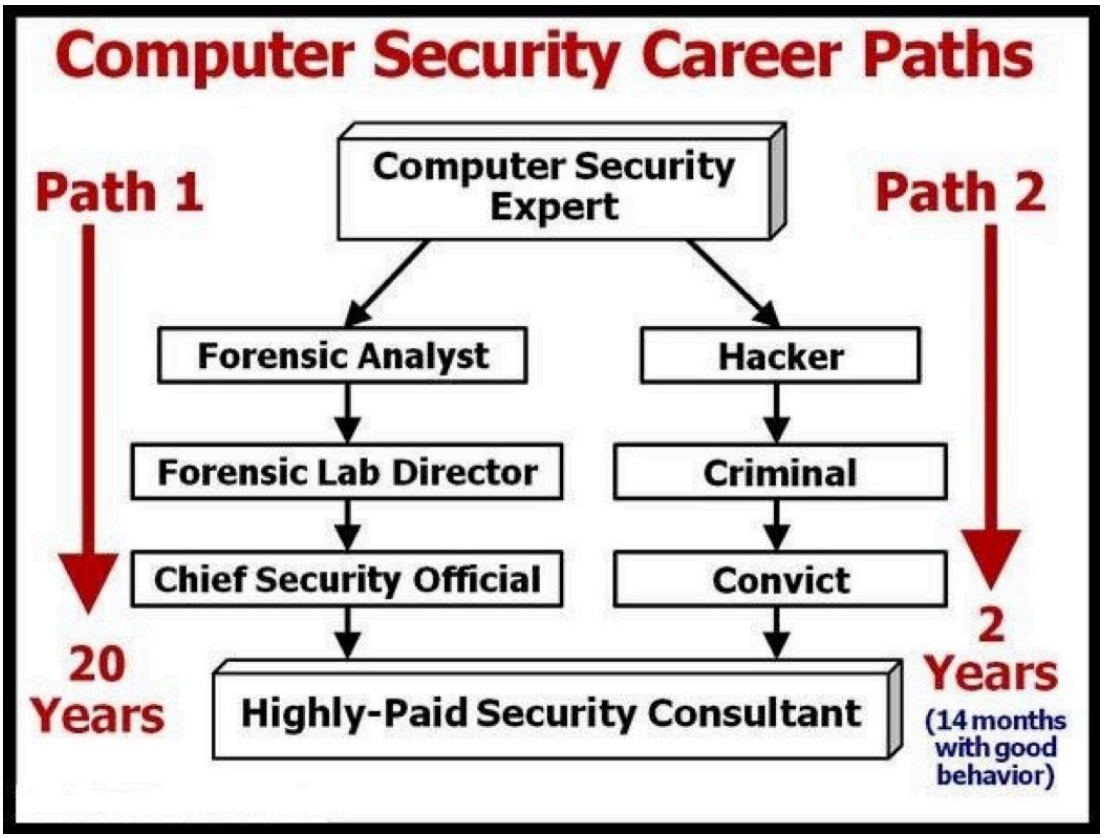
Because of these reasons, we would like to make a suggestion to consider the next time you are preparing for choosing your next RAM capturing tool:

1. The tool must have a single function: to dump RAM
2. Portability
3. Kernel-mode operation
4. Least possible footprint

You can find a number of utilities, which suits all these requirements, and all of them are free.

Career path—the choice is yours

Here in the DFIR or cybersecurity community, we are commonly faced with two career path options: spend twenty years building an excellent reputation and gain crucial experience to be a valuable customer consultant, or get off mom's couch long enough to become a young "hacker" and criminal. The second option, could ultimately lead down a path to becoming a weapon—a defender of the cyber domain, all before moving out of the basement.



Speaking hypothetically, if you would have known 20 years ago that to become a "Highly-Paid Security Consultant" all you had to do was "Hack" something or someone important, become a criminal and spend some time in jail, would you have done it?

All jokes aside, if you have been in the DFIR community for some time and are finally approaching the role of a "Highly-Paid Security Consultant", congratulations on all of your hard work and dedication to making it to the top, we appreciate you.

A word from CEO

Dear reader,

I hope you had fun reading this book, but I also hope that you found something new, which may help you to be better in one of the most noble jobs in the world—the one to protect our fellow citizens. My Belkasoft co-authors and I tried our best to make the book both entertaining and useful.

If you like the book and would like to read more from us, subscribe to our updates using the links below.

Yours,

Yuri and the Belkasoft DFIR Team.

Belkasoft

forensics made easier