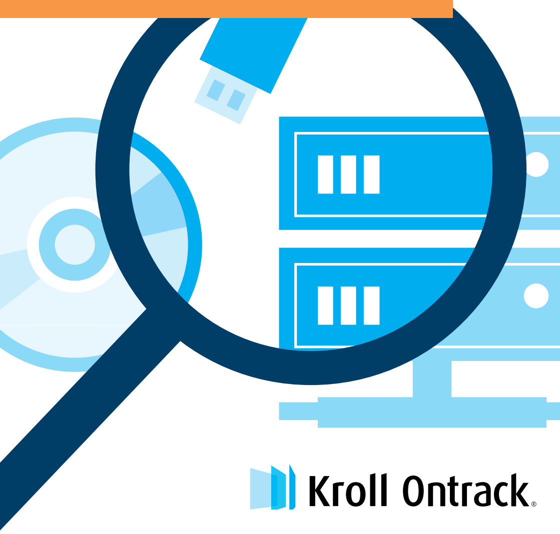
Computer Forensic Investigation



Kroll Ontrack®

What is it?

A computer forensic investigation is the capture, preservation, extraction and analysis of digital evidence, ensuring the integrity of the evidence is maintained so it will withstand legal scrutiny.

Forensic investigations are all about digital devices and as a nation, we are firmly welded to our tablets, laptops, mobile phones and PCs. Every time we take a photograph, send a message, open a document or plug in a USB drive, we leave some form of evidence trail. When these devices are misused, we use our expertise at Kroll Ontrack to locate the evidence and find the culprit.

An experienced forensic consultant will consider the following:

» **Where** the evidence is located

» **How** to access it

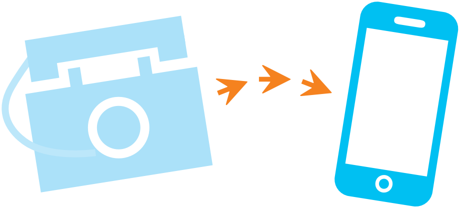
» **What** to do with the evidence

» **What** the evidence shows

It is extraordinary how quickly technology is evolving. The first phone call made on a mobile phone was in 1973, and 44 years later we can take HD photos, send messages across the world in seconds and we even have our own speech-recognition personal-assistant built into our Smartphones.

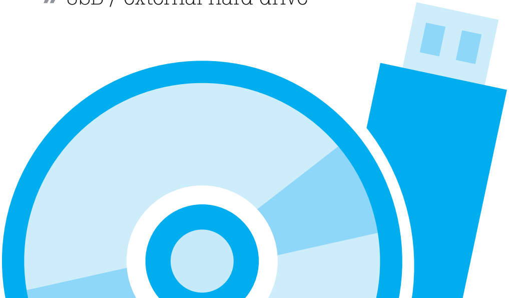
Faster still is the rate of upgrades for each device. We buy the latest handset and before we know it, 3 months later an even thinner and quicker version is being promoted.

However, one thing that remains constant is that these devices all hold evidence about what we have accessed, where we have been, who we have contacted and when we have downloaded a file. This is great news for a computer forensic consultant who will be able to access this evidence when a device is misused.



The typical types of media we investigate include:

- Laptop / PC
- Mobile Phones
- Server
- Back-up tapes
- CDs
- iPods
- Tablets
- USB / external hard drive



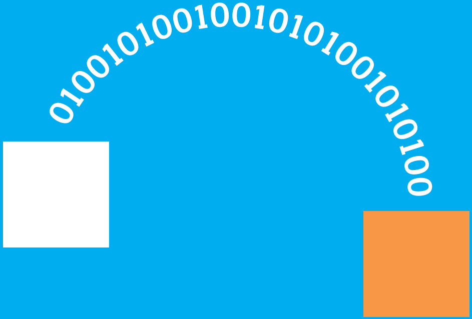
Whilst there is no typical computer forensic investigation and each will have unique characteristics and challenges, classic scenarios in which a computer forensic investigation will be required include:

- Internal IP/data theft
- Employment dispute
- External breaches/intrusion
- Query into the provenance of documents
- Computer misuse
- Harassment or bullying claims
- Fraud
- Criminal investigations (for the prosecution or the defence)

Case Studies

Intellectual Property Theft

Company databases were suspected of being transferred out of the client's premises. Kroll Ontrack performed 'imaging' (forensic bit-by-bit copies) on a number of PC's and laptops to ascertain which individuals had been accessing privileged information and copying it to USB drives.



Computer Misuse

Employees were suspected of accessing prohibited material on the Internet. Kroll Ontrack were able to image the hard drives and access the dates, times and levels of prohibited material accessed, leading to the conclusion, with evidence to prove this, that the material had been accessed during work hours.

Commercial Dispute

During the course of a dispute, Kroll Ontrack were asked to investigate whether a contract had been created on a company's premises on a specific date, and then if the printing function had been actioned by specific individuals. By investigating the company server and subsequently imaging the individual's hard drive, Kroll Ontrack were able to show the provenance of the document and ultimately prove that the document existed on the PC during the dates specified, and that it had been created and printed by the user in question.

Data Volumes

So what did we use to store data before technology was so easily accessible? Well, we used paper and lots of filing cabinets. It has been claimed that every two days we now create as much information as we did from the dawn of civilization up until 2003, approximately five exabytes (1 billion terabytes) of data. As technology has evolved, we have moved away from paper and now store information electronically.

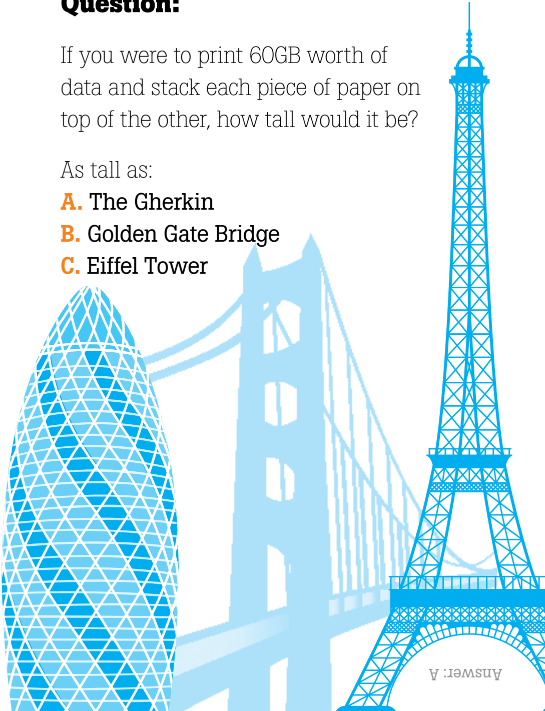
Why? The answer is that a) we trust technology, it's easily accessible and there are different methods to store data and b) that's a lot of paper!

Question:

If you were to print 60GB worth of data and stack each piece of paper on top of the other, how tall would it be?

As tall as:

A. The Gherkin
B. Golden Gate Bridge
C. Eiffel Tower



Answer: A

Technology saves the day

How much data do our laptops and mobile phones really hold? Well, just taking one photograph with a mobile phone would provide us with at least two pages of metadata (data about the photograph). This metadata could say what date and time the photograph was taken, what location you were in when you took it and can even show which direction you were facing (depending on the settings on your phone.)

Law firms and businesses that have thousands of documents often use an ediscovery platform to manage and review the documents. These platforms are built to quickly and effectively allow businesses to find relevant documents and include powerful searching tools and data analysis tools.

Case Study

A client contacted Kroll Ontrack regarding a potential IP Theft investigation. Two employees had left the business and the CEO had been informed they were starting up their own company – making them a competitor. Understandably the CEO was concerned and wanted to make sure company data hadn't left the business. So Kroll Ontrack imaged the two laptops and extracted the data and used a variety of forensic software to locate the evidence. It was clear that a lot of confidential data had been transferred between corporate and personal emails. Due to the volume of emails and files involved, we advised our client to use our ediscovery platform to locate the relevant data more effectively and quickly.

Litigation is now underway and the two individuals have a lot of answering to do.

Just because you can't see it – doesn't mean it's not there…

Maybe you've clicked on something you probably shouldn't have, or you have been looking at holidays whilst at work when you shouldn't be. Perhaps it's your partner's birthday soon and you know they will be snooping around online to see what you're planning on buying them, so you delete the Internet history. For whatever reason, we've all been guilty of deleting our Internet history. The question is, even when we delete a folder and then delete again from the recycle bin, is it really deleted and never to be seen again? The best way to think of deleted data is to remember the analogy of the lazy librarian.

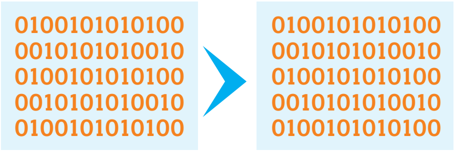
The lazy librarian, who upon being instructed to remove an unwanted book, instead simply removes the index card but leaves the book on the shelf, so the book is still there but no one has any way of knowing where to look. At some point in the future a new book is required to fill "the space" where the old book resides, the librarian now simply pushes the old book to the back of the shelf, now it is slightly harder to find (as it has a new book in front of it) but it is still lurking there on the shelf, if you were to look. In a similar way, deleted data remains on storage media in whole or in part until it is overwritten by ongoing usage or "wiped" with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers or other metadata relating to the deleted data may remain on the computer.

Forensic Analysis

Kroll Ontrack's digital forensic experts gather electronic evidence and materials in a forensically-sound manner as the foundation of a potential computer investigation, or for future use. Leveraging experience from thousands of data collection projects, Kroll Ontrack determines the most efficient and cost-effective data collection strategy for identifying digital evidence and gathering electronic data for forensic analysis or electronic disclosure. This will involve a process called 'imaging' where a forensic copy of the electronic device is taken and examined, leaving the original untouched.

Data must be collected in a forensically-sound manner to ensure the data is preserved correctly and most importantly, to ensure all metadata is retained and unchanged. Kroll Ontrack employs robust collection methodologies ensuring data handling methods are defensible, repeatable and able to withstand legal scrutiny in the event of court proceedings.

After we have taken a bit-by-bit copy of the hard drive (imaging) we will begin the investigation of the imaged copy leaving the original media untouched and preserving the data.



Depending on the nature of the case, the computer forensics investigator will carry out an investigation on the device(s) of concern. As required, this imaging process can be executed on, or off-site. A detailed examination of the imaged data is then performed, examining both visible and invisible data, including data that any wrongdoer may have sought to erase or delete from a live system.

A computer forensic investigator will then prepare a report, as required, in the expectation that it may be used as evidence in legal proceedings; and that he / she may potentially be required to attend court in order to give oral evidence.

So what can a Forensic Analysis show?

- Deleted data – whether data has been deleted and information about that deleted data, including in certain cases the deleted data itself
- Information about USB connectivity (in other words whether or not memory sticks have been inserted into a device and had data copied to them)
- Web based communications, Hotmail/ Yahoo/Gmail – whether these have been used to send emails
- Web based storage applications (Dropbox) – whether data has been sent to these locations and information about when, what etc.
- The results of key word searches run across a device

Using a combination of software and forensic skill, we are able to forensically search data for keywords in order to locate relevant information. For example, once we have imaged a hard drive, we will upload the data into our software. This software will divide the data into the appropriate categories such as social media sites, web chats, cloud services and even dating sites. After that we can target certain data sources and run the searches.

Back-up tapes

Tapes contain a snap-shot of data which were present on a system at one time. This could include information which is no longer available in 'active' storage. Say for example, an employee had tried to delete incriminating information from the live system; we would be able to recover this information by forensically examining and extracting data from the tapes.

It is always important for lawyers to ask their clients what back-up software their business has in place. Tapes are a valuable source of legacy data, they are often forgotten about as they are stored offsite and employees aren't aware of their existence.

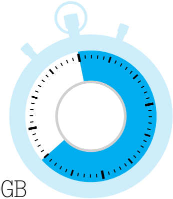
Back-up tapes come in all shapes and sizes, the important questions to ask the client include what type of tape was in use at the relevant time and what type of back-up software was used. Kroll Ontrack has over 300 tape drives in order to extract the data. However, sometimes we will need to build the environment in order to extract the data and this is often very time consuming.

Types of tapes:

- LTO
- DLT
- DDS

Frequently asked questions

How long does it take to image a hard drive?

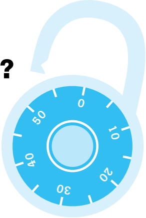


It usually takes between 4 to 6 hours to image a typical 500GB hard drive. Computer forensics is an art and a science and takes time and expertise to carry out procedures. If you have watched programs such as “CSI” or “Law and Order”, you may think forensic consultants are able to solve every case within an hour, including adverts. Unfortunately this is not the case and because of shows like this, we have created our own definition called the ‘CSI effect.’ It is important to understand that computer forensics is much more than what is seen on TV. Not many cases are done in an hour and if they are, it’s probably not been done properly.

Can we recover data from the Cloud?

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. It is technically possible to recover data from the Cloud provided the correct contractual provisions have been put in place with your cloud provider allowing you to access your data, especially when it is stored with other clients’ data, The key issue here is to ensure that you can have access within a reasonable time period to your data.

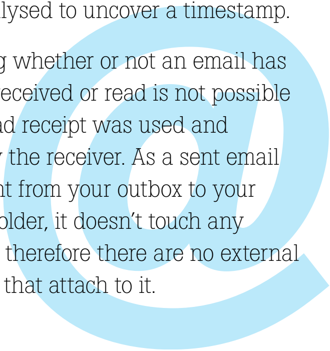
Can you crack passwords?



The ability to crack a password depends almost entirely on the password and in many cases, we are able to determine a user's password. We can use "Rainbow Tables", "Dictionary Attacks" and forensic tools to attempt to overcome passwords. However a sufficiently strong password is exceedingly difficult to crack in a reasonable time frame. In the password world, length is key. There are only 10 numerical values and approx. 20 symbols on a keyboard, so adding one to the end of a basic password does little. If a phrase that combines words such as "THEMERRYWIVESOFWINDSOR" or a series of unconnected words "HORSESTAPLEBATTERYGOAL" has been used, it may take hundreds of years of "brute force" to crack.

Can you tell me when a specific email was sent or received?

Generally, a received email will contain some metadata from which we can determine its provenance. When the email left the sender's email server, bounced around the Internet and landed in your email server, data about this path is created within the email record which may be analysed to uncover a timestamp.



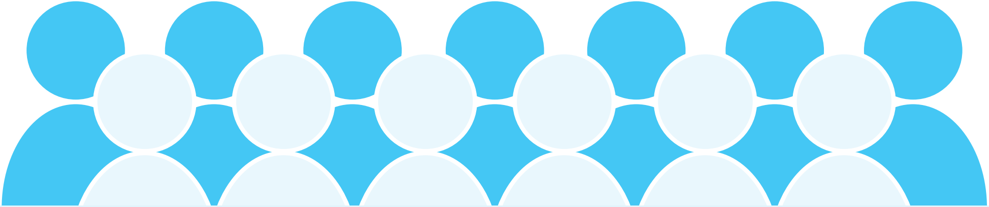
Determining whether or not an email has been sent, received or read is not possible unless a read receipt was used and accepted by the receiver. As a sent email goes straight from your outbox to your sent items folder, it doesn't touch any servers and therefore there are no external times/dates that attach to it.

Can you extract data from a mobile phone?

Whether we can recover data off a mobile phone depends almost entirely on the make and model of the phone. The forensic industry is constantly playing catch up with new operating systems and proprietary file storage systems on mobile devices. We use a range of tools and techniques to increase the likelihood of extracting the relevant data, however, a good initial guide to whether your handset is supported for extraction is freely available at www.cellebrite.com/mobile-forensics/support/ufed-supported-devices.

Want to learn more?

Kroll Ontrack offer two main training and education seminars:



First Responder Training

First Responder Training is designed for frontline technical staff who, in response to a computer-related incident, are responsible for the initial preservation of the digital environment that may require further forensic investigation. The course assists key personnel to understand and recognise situations where digital evidence may be relied upon, understand the key types of data that reside on live systems, become familiar with the laws pertaining to the acquisition of computer-related evidence, correct computer forensic principles including the ACPO guidelines as well as guidance on the key issue of how to ensure chain of custody and evidential integrity. To this end, success requires that appropriate understanding and procedures are in place to cover a relatively rare, but complex, event. Kroll Ontrack's First Responder Training will provide you with the tools and knowledge to respond appropriately.

Forensics for Lawyers

Forensics for Lawyers gives solicitors, barristers and other fee earners an overview of the risks, issues, responsibilities and requirements a client may face when encountering a situation where a computer investigation is required.

It also outlines the high level processes to be followed when clients are faced with the need to gather electronic evidence and the possible consequences of not following appropriate procedures.

Lawyers from all practice areas will benefit from a greater awareness and understanding of the processes and risks involved.

The seminar provides lawyers with an overview of:

- How to recognise a forensic requirement – typical / common types of investigations
- Changing data landscapes – e.g. mobile devices, social media and cloud computing
- Where to locate evidence – e.g. data mapping and cataloguing
- Computer forensic principles – ACPO guidelines
- Other wider business issues to consider – self-reporting to authorities, media announcements etc

Typical cases involving electronic evidence include intellectual property theft, inappropriate use of the Internet, fraud, competition/anti-trust, employment disputes and much more. In these situations clients look to their legal advisors to help them act quickly to protect themselves and secure any potential evidence. Our training will enhance your knowledge of the issues relating to electronic evidence and improve your team's ability to advise clients about computer forensics issues.

By gaining a sound level of forensic awareness, your clients will benefit from having an advisor who understands the appropriate processes, working practices and skills that are available to cover these increasingly common and complex events.

Ediscovery.com/UK

Ediscovery.com/DE

Ediscovery.com/FR

Ediscovery.com/NL

Ediscovery.com/EU

Contact Us

Kroll Ontrack
Nexus, 25 Farringdon Street
London EC4A 4AB
+44 (0)20 7549 3870
enquiries@krollontrack.co.uk
www.ediscovery.com/uk