Introduction

Have you recently been involved in events or transactions which are now disputed and evidence for which may exist only on a computer, tablet, smart phone, remote website or computer system owned by a large business or government entity? Are you a cyber victim?

Think about the number of transactions you have been involved in over the last few days – the chances are that the majority have had some digital element – phone calls, text messaging, Internet web and app activities, credit card purchases, interactions with large organisations, banks and public authorities, or emails in which promises were exchanged and contracts created. Have you relied on what a website says, or have you had made apparent promises on a website, via social media or other Internet service? Have you had concerns over what is being said about you on a website or social media service? Do you use a VOIP service like Skype – would it be useful to have a reliable record of what was said?

What evidence exists that any of this took place? And is the evidence strong enough to overcome objections from the person or organisation that could become your opponent in legal proceedings?

Have you been involved in an accident and taken digital photographs or video of the aftermath, perhaps for use in an insurance claim? Did you receive a defective product and want to use a photograph to obtain redress? How do you ensure that these still and moving image files become unquestionable evidence?

Think also about situations where you believe yourself to be a victim of a crime and where part of the activity took place in and around computers, mobile phones and Internet facilities – frauds of all kinds, identity theft, harassments, bullying, discrimination, blackmail, industrial espionage, the unwanted receipt of illegal material such as images of sexual abuse. What would you be able do to trace the perpetrators if you were victimised by malware, a Trojan or a Distributed Denial of Service? Will you want the benefit of a photograph or video taken with a digital camera, or something caught on a CCTV system? How easily would you be able to deliver helpful and reliable evidence in digital form – or respond to law enforcement requests? Whatever you think "cybercrime" is – and there are many different definitions – remember that digital evidence can be critical in the investigation of many "ordinary" crimes.

Digital evidence is being created wherever we go and is often essential to resolving disputes and attributing blame for crimes. In "advanced" countries an *average* household may own over seven digital enabled devices; some individuals may own more than that just by themselves.

We create digital traces of our activities on devices which we own – computers, mobile phones, tablets – on remote "cloud" services, on the computers of those who employ us, on the computers of large organisations, commercial companies and governments as we interact with them, and they are also recorded almost without our being aware of them as we browse the Internet, as we visit specific websites, use social media, via retail shop systems, on bank ATMs, as we pass by closed-circuit television cameras and as we travel on public transport. If you use a digital camera, digital cctv or take pictures on your smart phone those too are – digital. And of course everybody else is creating digital evidence on devices they use – and in particular circumstances their existence may be very useful to you.

But these are simply records which exist somewhere on some computer or other digital device. To turn them into evidence, something sufficiently robust and reliable to persuade the courts, is another matter.

The existence of some of the most important evidence sources may not even be particularly obvious – they may be log and event files, or features designed to aid recovery after a disaster, or hidden facilities in web browsers and email programs – and which, if identified in a timely fashion and carefully preserved may of great value to a technical investigator.

And many of these issues apply also to businesses. Indeed, as an expert witness called in to help in civil as well as criminal cases I frequently find that neither party has properly collected and preserved potential digital evidence. Quite often the cost of a full forensic examination to look further for useful traces in the available computers will exceed the sum in dispute. The parties then have to make some messy compromise of a settlement. Costs in civil disputes also include the obligations of disclosure/discovery – the requirement to produce material of possible use to an opponent - these too can easily be under-estimated.

The purpose of this ebook is to provide a primer and handbook on digital evidence – how to acquire and preserve its various forms safely and reliably, and how to use them to resolve disputes and participate in and support investigations. Contrary to what might be thought, there are many useful activities that can be carried out without having specialist "computer forensics" skills. But you also need to know when to call in the specialists and what to ask them to do.

As a result, this ebook at some points tells you "how to" and at others provides descriptions of "how it's done".

I have concentrated on evidence which is likely to be immediately available, even if its presence is not instantly obvious. At various points evidence may have to be obtained elsewhere, from third parties and on the open Internet. There is a separate subject called Open Source Intelligence which deals with the many sources of information that are freely and legally available. In general terms I don't cover these, for two good reasons – this ebook would have to double in size and, more significantly, there are some excellent existing books on the subject already out there. But where appropriate I do describe some valuable tools and techniques for capturing various types of open source material, particularly in relation to web-pages, social networks, texts, emails and IP address tracing.

It is a reference book rather than something to be read from cover-to-cover (or rather, end-to-end) and use has been made of convenient ebook facilities which enable the reader to move around the text clicking on links, hopefully corresponding to immediate problems. Sometimes the same piece of information, though slightly differently expressed, appears in more than one place.

Do not feel you have to read the whole of the book – read this introduction and a few of the early sections and then dip and search for the information that will help you. Some sections are quite long, others very short. Some sections are relatively "basic" others more "techie"; you as an individual may not need to understand all of them. In the same way other sections are more focussed on legal situations and again you as an individual reader may feel you don't immediately need all of the detail.

The longest section is on smartphones – because they are now the single most important source of digital evidence and also because of their interior complexity.

The book is not aimed at those who specialise professionally in digital forensics; rather it is for everybody and anyone who find themselves in a contentious situation and who strongly suspects that evidence to resolve the problem may exist somewhere in digital form. In practice most people and nearly all businesses will find that they need to rely on questioned digital evidence several times in the course of a year. The event may be as trivial as a disputed transaction, a question whether an email was sent and received, whether a document or file has been altered and tampered with, whether to trust a digital photo, or on a grander scale, suspicion of a serious crime. Digital evidence is equally for those who hope to locate and rely on it and for those against whom it is being used.

People in this position soon come across a barrage of problems, for example:

- the simple printout of an email is rejected because it is too easy to forge
- recalling a webpage because there is interest in its content or because it was used for a transaction turns out to be far from straightforward
- a quick "look" on a computer or smartphone to discover what was on it results in a complaint that the whole of the evidence from that computer has become unreliable because your activities have caused contamination
- there is a dispute that a text message was sent and received
- actions which may be easy to achieve by the simple use of technology can turn out to be illegal, resulting in some instances in the exclusion of evidence from legal proceedings while others may be criminal offences
- a quick examination of someone else's computer or smartphone without their consent gives rise to a criminal complaint of computer misuse and further complaints of invasion of privacy
- employers who carry out computer and network-based surveillance of their employees may find that although easy to execute their actions have generated a whole raft of problems
- big organisations insist that their computers never fail but nevertheless your own recollection of events is rather different; getting sufficient means to be able to test the reliability of those big business computer systems may prove difficult
- and so on

If you are currently involved in circumstances where you think digital evidence is likely to be important and have bought this ebook specifically for that purpose – you will find an Emergency Investigation Check List you need to take.

The basic assumption I have made about you as a reader is that you are reasonably comfortable with the regular daily use of your computer, tablet, smartphone and can carry out basic administrative tasks. Many of the most frequently used procedures described here require a calm head and a methodical approach rather than unusual technical skills. Most of the detailed examples are given in terms of the Microsoft Windows environment as that is overwhelmingly the most popular platform, but where appropriate and helpful I also refer to OSX/macOS for Mac devices and Android and iOS for smartphones. But many of the underlying principles are the same no matter what operating system is being used.

The arrangement of this book is as follows: there are some fundamental concepts to grasp about evidence in general and digital evidence in particular. Some of these concepts relate to technology and in especially the challenges of

dealing with the basic raw material of digital evidence, data. Digital data is nearly always highly volatile and easily contaminated, accidentally or deliberately.

Once these fundamental concepts have been set out, the rest of the book deals with specific situations and specific types of digital evidence and does so in as practical way as possible. I have selected topics and related names for the sections corresponding to what I hope will be the most common types of queries people will have. These are designed to be read on an "as needed" basis. You will find a number of internal links to click on.

The specific situations fall into a number of categories, for example:

- Things you can do yourself as an individual and in relation to devices – computers, tablets, phones etc. – which you yourself own
- Things you can do yourself as an individual and in relation to devices – computers, tablets, phones etc. – which you yourself own but where you may require some specialist assistance
- Things in relation to devices – computers, tablets, phones etc. – which you yourself own but which only a specialist can do for you. This is mostly the territory of digital forensics, advanced data recovery and event reconstruction. You may need to consider whether these investigations are likely to be productive and value for money.
- Situations in relation to devices – computers, tablets, phones etc. – which you yourself own but which require specialist intervention – but where you need to undertake the necessary preparatory work to identify and preserve material for the specialist to work on.
- Where you need to acquire information from a public electronic source such as a website or social media site
- Where you need to acquire information relating to you from a remote electronic source such as a website but to which you have appropriate authorisation to access
- Where you need to acquire information relating to you from a remote electronic source such as a website but to which you do not have appropriate authorisation to access
- Where you must obtain information from an employer
- Where an employer wants information from you
- Where you need information from potential counter-parties to litigation
- Where you need information from third parties such as separate businesses, including financial institutions, telecommunications companies and Internet Service Providers
- What happens if your equipment is used partly for business and partly for personal private use, what is sometimes referred to as BYOD, Bring Your Own Device.
- What happens if in respect of a device you wish to have included in potential legal proceedings, there are arguments that all or part should be excluded on

the grounds of privacy, commercial confidentiality, legal professional privilege or state security.
- How to deal with encrypted material – material that you control which others demand access to, and material created and encrypted by others but which you wish to see
- How, during litigation proceedings or criminal investigation, to respond to e-disclosure/e-discovery obligations and "production" orders
- Where what you need will only be released after a Court Order – and what information you may need to supply in order to get an Order granted.
- Techniques and levels of access to data sources only available to law enforcement and other official investigators

As a result, the audience for this book is rather diverse. If you think about it, in most litigation situations at least two lots of people / entities are likely to be interested in the same item of potential evidence – and each needs to know what the other can or should or could be doing.

It is unlikely that any single individual will need to read every section of this book; however it is convenient to have all the material together in one place.

Thus at various points the audience could be:

- Private individuals, consumers
- Businesses and other organisations
- Individuals employed as support technicians in businesses and organisations - and in particular those who are designated "first responders"
- Security professionals
- Professionals who advise individuals and businesses – these can include accountants and private investigators
- Law enforcement officers
- Others in the public sector charged with carrying out investigations
- Civil and criminal lawyers who advise any of the above
- Prosecutors
- Judges
- Any of the above who need to employ or interact with specialist digital forensics technicians and need to know what you can ask them to do – and understand some of the concepts and terminology that the specialists may use.

I also expect there are people who will find the mechanics of digital investigatory techniques inherently interesting.

Please also note that evidence is simply an essential requirement to settling a legal dispute; this book is about acquiring reliable digital evidence – not about addressing entire specific litigation or prosecution situations.