Emergency Investigation Check List

Most people will not be prepared for the need to collect digital evidence. Events will have sprung on them unexpectedly. The danger is that much of the energy will get transferred into anger, panic and worry rather than a calm assessment of circumstances and a proper plan of action. Although this section is headed "emergency investigation check list" much of it is about imposing a discipline on activities. You need to have a sharp focus on what your overall aims are. One aim is presumably to stay in business; if your business is in the least computer-dependent that means some sort of conflict with the ability to collect evidence in “ideal” circumstances. Another aim will be to ensure that you can continue to use your computer facilities, or at least have access to all your most important data.

Among the risks you have to worry about are: that premature un-thought-through activity in fact destroys potential evidence; that your need to acquire reliable evidence often requires you to de-power computers upon which the life blood of your business depends; that you are breaking the law; and that the costs of acquiring the evidence outweighs any benefits from "winning" your case. But evidence acquisition will be one of your aims because it is the root to financial recovery, to limiting your own exposure, to getting an insurance payout, to assisting law enforcement: you will need to be identifying potential evidence which will support these aims.

Be aware of your own limitations and don’t try and be a hero in order to be helpful to others or to “solve” what appears to be an immediate problem. As far as possible keep on asking yourself – if I make a mistake will I be able to rectify it? This is particularly important if you are handling original material, as opposed to copies.

Not all of these elements will apply in every situation, but you should consider each one, if only briefly, to make sure which you can safely ignore:

1. **Start an audit file/diary of decisions and actions.**

   Decisions - because you will have to make choices between various courses of action and you may get questioned about them later. **Actions** - the activity you decide to carry out. One key advantage is that it forces you to think through what your objectives are, what sort of evidence you may need and where it is likely to be located. It is also a bulwark against criticism – with the benefit of hindsight it is often possible to say that a particular course of action is wrong; and if you are to be criticised at all it must be on the basis of the circumstances as they actually appeared to you at the time.

   Ideally the audit trail should carry with it date and time stamps for each activity and decision. It doesn’t matter if you embark on a course of action and then decide you have got things wrong – the fact that you are recording events adds to the credibility of your overall testimony.

   The remainder of this list is not sequential – many of the items interrelate.

2. Identify your aims; what are the issues the evidence needs to address?

In simple cases the issue in contention may appear to be so trivial as to be not worth setting down but a simple statement along the lines of "The website did not record my activity properly", "I did not get a proper acknowledgement of my transaction", "I sent an email which someone says they never received", "I placed an order and arranged the payment but never received the goods or service should"; "This web-page / social media posting causes great offence / is defamatory / contains obscene material", "I need to get hold of an important document and be able to authenticate it", "I have some photos or video which show what happened, or the immediate aftermath" , "I think I have been hacked" helps you focus your mind on what you are seeking to achieve.

This business of identifying your aims becomes all the more important if you find you have to spend significant amounts of time or, worse still, significant amounts of money on external help. There is a good maxim from the civil courts – "costs must be proportionate to the sum in dispute".

3. Constantly Revised Risk Analysis

As you will have seen already, in all but the simplest of circumstances you will have to make decisions: preserving evidence "perfectly" while still carrying on using the device where it is located because it is essential to your life-style or business; deciding whether a course of action to capture evidence form or about some-one is both "necessary" and "proportionate"; whether a potentially expensive course of action is in all the circumstances justified. If issues are complex – what are the likely costs measured against the sum in dispute or the harm you wish to mitigate? And so on.

These risks will keep on changing and so may your assessment of them. So keep thinking about them – and where appropriate, record your decisions in that diary / audit log mentioned in Item 1 above.

4. Do you need / have access to legal advice?

There are many forms of activity in relation to the collection of digital evidence which are trivially easy to accomplish but which are either directly illegal or may give rise to counter claims by those from whom you have collected the evidence. If you are an employer, or acting for one, you may need to have regard to the rights of an employee even if they are suspect. There may be limits to the amount of information that you can collect in relation to individuals. Elsewhere in this ebook there is a fuller discussion. But unless your requirements of a very simple nature

you should at least need to bear in mind is the need to have access to reliable legal advice. Please check out the Legal Basics section.

5. What sorts of evidence are likely to be helpful?

Once you have determined your overall objectives you need to consider where evidence to support your claims might be found. Are you looking for emails, for web activity, for specific documents or files, or for something else? Again elsewhere in this book you will find useful advice.

6. Will you be able to link the evidence to specific individuals – and if so, how?

Where a computer or a system is being used by more than one person you may need to anticipate that your suspect or adversary will deny that they were responsible for the specific item of evidence – you need to think how you might be able to overcome this objection. There may be log files of various kinds that can help pinpoint authorship and attribution.

7. Where, physically, are the evidence sources located?

Almost certainly in the first instance you will be thinking of generic categories of evidence as held on a computer – email archives, substantive documents, web activity etc. You now need to think about the physical location about evidence as a precursor to acquiring it safely. In many simple situations the evidence will be held on a personal computer or smart phone which you yourself own, in which case there is very little problem. But it may be that the real evidence is held on corporate facilities, may be in some backup, or perhaps on a cloud service. Perhaps there is more than one source – for every email there is both a sender and recipient. If you are carrying out of transactions with a website then there may be a record on your own computer but they should also be one or more on the remote website; if money has been involved there are likely to the records either with the banking or credit card service or with a payment scheme such as PayPal. For the moment you need to note that these other records exist even if it is not immediately obvious how you're going to obtain them easily.

8. How do you propose to extract the evidence safely? How much / how little do you need to take? Will you need to take live data – and what precautions may be appropriate?

Once the evidence sources have been identified you need to consider how you can extract the items you want without causing contamination. Elsewhere in this ebook there are pieces of specific advice. You may be able to do some of it by a simple "print" command or by copying out various files onto separate storage. But in the

case of emails it may be better to copy out a whole archive, in the case of web traffic although a "print screen" action can be very helpful it may also be sensible to try and capture the “Internet history”. The gold standard as far as personal computers are concerned is the forensic disk image which requires specialist hardware and software to be achieved safely. Depending on the circumstances, though, the cost of calling someone in to do that for you may be fully justified in terms of having a properly preserved snapshot of the state of a computer at a particular point in time.

In a few instances you may have no alternative but to try and capture live data – here the "print screen" command or the taking of a photograph of what can be seen on a monitor or screen is the best you will be able to do.

Capturing data held on a smart phone or tablet is often more complicated - you can’t “image” a phone or tablet in the same way as a personal computer as there is no equivalent of a removable hard disk. In addition, a phone is always on, ready to receive calls, SMSs, emails and other alerts. Specialist help is available but photos of the screen of the device – taken with a separate camera – may be better than nothing at all.

9. If you are working with a computer system that is keeping a business going or otherwise generating revenue

Calculate the implications of closing the system down temporarily while you extract evidence safely. In some instances the cost of removing a business’s lifeblood even for a relatively short time may be greater than any benefits you can derive from having reliable evidence. (This is one of the key decisions you will have to make and which should be reflected in the diary/audit log that you are keeping).

10. Once extracted and obtained, how do you preserve evidence against possible later change?

Digital files are highly volatile, potentially easily altered without leaving obvious trace. Your opponents may suggest accidental contamination or more seriously, deliberate manipulation.

There are a number of potential solutions – a computer hard disk , phone or tablet can be placed in a tamper-evident bag (sealed and tagged so that any subsequent opening leaves obvious traces) but that may be inconvenient if the device is important to some-one’s life-style or business. There can be specific problems with phones – if they are switched on they will be able to receive calls, messages and if they are smartphones, emails as well. But they may also be password-protected and once switched off, difficult to get access when powered up again. In addition, leave a phone switched on but in a radio-proof bag, and the battery may run down. But memory cards can be removed and placed in sealed envelopes. Perhaps there is some feature of a file which means that it can in any event be “trusted”. Later we’ll see a number of these evidence preservation techniques.

11. What analyses, charts etc may be needed in order to make conclusions manifest?

Where the situation being investigated is more complex it may help if time-lines/chronologies are produced to show a sequence of events. Perhaps you need to show a course of action from which intent can be inferred. Or show a range of transactions.

There are plenty of low cost items of software from which charts and other graphics aids can be generated. There are also very expensive "link analysis" and "data aggregation" products used by professional investigators to plough through vast quantities of data and identify patterns.

But as a first responder to events you need to consider whether you may need to resort to chart production. If so, you need to think about which items will be needed to make the chart useful – and to ensure that each element is evidentially reliable.

12. Will you need specialist assistance, for data recovery, event reconstruction?

Do you need professional digital forensics advice – in relation to acquisition, preservation, subsequent analysis? This ebook is principally about things you can do yourself. But there will be situations where your skills and resources are simply inadequate. The beginning of this chapter warned against the desire to be a hero or to get quick solutions. In the detailed chapters that follow you will get an idea of the various types of help and skill that are available in the market-place.

There is a separate section on instructing experts.

13. Disclosure / Discovery obligations

It can be a surprise to those entering litigation that they have obligations to their counter-party to disclose any material they hold which might assist the counter-party's case or weaken their own case. In most jurisdictions the obligation is to identify and list such material but not to deliver it unless requested.

A related obligation is to take steps to see that the material is not destroyed; any deliberate destruction is likely to be regarded very adversely by a court, often to the point of deciding in favour of an opponent.

14. Any ethical /PR issues?

Although you may be satisfied that all your actions of fully legal they may still look bad at in the eyes of third parties. This is particularly true when you had to mount

what amounts to a surveillance operation. You need to consider how your actions of viewed by others and if you are prepared to justify them.

Although this is designated as a checklist you should bear in mind that this is not a list of things to do one after the other, rather many of the headline items will cause you to have a review of other activities in the list. For sample the ethical and PR issues and the cost implications will need to be in your mind throughout.

Investigatory Stages:

Formulation of Aims	What is the overall situation / legal proceeding you wish to try and resolve?
Identification of Potential Evidence	On what devices, in what locations and in what forms do you think evidence might exist? Are there any legal constraints?
Safe Acquisition of Evidence	To avoid contamination during collection; to ensure that you have all that is relevant
Preservation of Evidence	To avoid subsequent alteration of evidence
Analysis of Evidence	Examination, methods, inferences, conclusions
Presentation of Evidence	Preparation of statements, exhibits etc. for use in litigation etc.