View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Open Research Online

Open Research Online

The Open University's repository of research publications
and other research outputs

Chapter 7 - Procedures at Digital Crime Scenes

Book Section

How to cite:

Kennedy, Ian and Day, Ed (2016). Chapter 7 - Procedures at Digital Crime Scenes. In: Bryant, Robin and Bryant, Sarah eds. Policing Digital Crime. Farnham, Surrey, UK: Ashgate, pp. 147–160.

For guidance on citations see FAQs.

© 2014 Robin Bryant; 2014 Sarah Bryant

Version: Accepted Manuscript

Link(s) to article on publisher's website:
https://www.routledge.com/Policing-Digital-Crime/Bryant/p/book/9781138257443

Copyright and Moral Rights for the articles on this site are retained by the individual authors and/or other copyright owners. For more information on Open Research Online's data policy on reuse of materials please consult the policies page.

oro.open.ac.uk

This is a draft manuscript of a book chapter published by Routledge in Policing Digital Crime on 2014, available online: https://www.routledge.com/Policing-Digital-Crime/Bryant/p/book/9781138257443

Chapter 7 Procedures at Digital Crime Scenes

Ian Kennedy with Ed Day

Many readers will be familiar with the role of the 'crime scene investigator' (previously known as the 'Scene of Crime Officer', or erroneously as the 'Forensic Scientist') who specialises in locating and preserving evidence at a crime scene. In principle, their training and experience allows them to identify the best places to look for, retrieve and (to a lesser extent) analyse and interpret traditional forensic evidence, such as fibres, DNA and fingerprints. However, for criminal investigations in the UK involving digitally-based evidence, this role is performed by what is typically termed a 'first responder' (or 'digital evidence first responder', a DEFR) from a police force's Digital Forensics Unit (DFU), or a unit with a similar title. In the UK police officers will receive training to act as first responders as part of their initial training (see chapter 6 and Bryant et al., 2013), but often this role is usually performed by other police staff. The initial role of the first responder is to recognise the sources of digital evidence that may be relevant to the subject under investigation. Note however that procedures at digital crime scenes are inter-connected with the analysis of digital information and evidence, which is examined in Chapter 8.

The 'forensic practitioners' is a collective term for both the first responders and the forensic investigators (or 'digital evidence specialists', the DESs) within a DFU, although in some forces the investigators might also act in the role of first responders, at least from time to time. The forensic practitioners may be warranted police officers or other police staff; the balance varies between forces.

In the UK a lawful search for evidence is typically performed under Section 18 of the Police and Criminal Evidence Act 1984 ('PACE') and evidence is typically seized under Section 19. If the forensic practitioner is not a police officer, his or her name will usually appear on the search warrant.

As for any crime scene, an entry plan is likely to be created before arrival if time permits. The plan often includes an assessment of any potential disruption caused by search, seizure and other activities, for example how the seizure of a company's server would damage its business. Any relevant warrants will be obtained prior to arrival at the scene (Britz, 2004). A power to search for evidence is provided for under PACE section 18. The PACE Codes of Practice also apply.

The potential digital evidence likely to be encountered by first responders is many and varied. In effect where there is the capability for storage or communication of digital data is of interest. Locations include (but are not limited to) digital storage media used in PCs, Macs, tablet computers (hard drives, solid state drives), memory cards, USB pen drives, optical and magneto optical disks (CDs, DVDs, DRAM, Blu-ray),smartphones and mobile phones, Personal Digital Assistants (PDAs), mobile navigation systems (Satnavs), digital video cameras (including CCTV) and networks (see chapter 9).

Principles and guidelines for attending digital crime scenes and collecting digital evidence

There are a number of sets of national guidelines underpinning principles for attending digital crime scenes and the collection of digital or electronic evidence together with developing international standards.

Perhaps one of the better known examples of a set of principles are those from the Association of Chief Police Officers (ACPO) for England and Wales. There have been a number of iterations of the ACPO guidelines (although the underpinning principles have remained largely unchanged) and the latest edition of the guidelines ('the ACPO Good Practice Guide for Digital Evidence') was released[1] in March 2012. The guide outlines four overarching principles that should be followed in any digital investigation (ACPO, 2012, p.6) and the principles are worth quoting in full:

'Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

[1] http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf [Accessed: 11 February 2013)

Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to'.

These are sound principles to follow when dealing with digital devices and data, and we will see how they can be applied to investigations in this chapter and chapter 8.

There may appear at first sight to be a conflict between the first and second principles; the first principle requires that original data must not be altered, whereas the second principle refers to accessing the original data. The problem arises because it is highly likely (unless certain precautions are taken) that the original data will be altered in some way when accessed. For example, the process of logging on to a windows-based PC will change the data because a record of the logon will be recorded in the windows registry (amongst other places). So if an investigator is unable to adhere to the first principle (ie the data is probably being altered) then the second principle must be followed – the person must be competent and able to give evidence concerning the consequences of their actions.

In the US the Department of Justice (DoJ) have produced a guide for law enforcement agencies on the forensic examination of digital evidence which includes recommended actions at a digital crime scene (although these guidelines date from 2004). These are similar in nature to the ACPO principles cited above. For example, the DoJ guidelines require that '[a]ctions taken to secure and collect digital evidence should not affect the integrity of that evidence'; that '[p]ersons conducting an examination of digital evidence should be trained for that purpose' and that '[a]ctivity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review' (National Institute of Justice, 2004). However, in the US the Federal Rules of Evidence (in particular 'Rule 702: Testimony by Expert Witnesses', much of 'Article IX: Authentication and

Identification' and some of Article X: Contents of Writings, Recordings and Photographs') apply as much to digital evidence as to more traditional forms and hence in effect the Rules provide a set of underpinning principles to guide digital crime scene actions.

In 2002 the International Organization on Computer Evidence (the IOCE) working in consultation with the G8 nations produced their 'Guidelines for Best Practice in the Forensic Examination of Digital Technology' (IOCE/G8, 2002). Section 7 of the guidelines describes best practice in location and recovery of digital evidence at the scene including anti-contamination precautions, searching the scene, collecting the evidence and packaging, labelling and documentation.

Finally, in 2012 a new ISO standard (ISO/IEC 27037:2012) was published dealing with '[i]nformation technology – security techniques – guidelines for identification, collection, acquisition, and preservation of digital evidence' (ISO, 2012a). Of particular importance where countries implement these standards will be section 5 where the principles are outlined, and section 6 which describes the key components of identification, collection, acquisition and preservation of digital evidence (including chain of custody), the precautions at the site of the incident, the required competency, roles and responsibilities of the personnel involved and what documentation is required (ISO, 2012b).

Possible locations for evidence

As noted earlier, devices such as computers, media, tablet devices, games consoles, satellite navigation devices, mobile phones, photocopiers and fax machines are all capable of storing digital evidence. The digital information of interest to a first responder and an investigator may be present wherever data is stored and processed, for example in any device with a microcontroller. It is vitally important for first responders to keep abreast of a rapidly developing field in which products of new technologies may be smaller or simply unrecognisable as sources of digital evidence.

The hard drives of PCs and the solid state devices within some laptops and mobile and smartphones, are obviously locations where a digital forensic investigator might locate relevant information, for example concerning preparations for committing a crime. Less obvious examples include modern washing machines whose programmable cycles use solid state memory, and which might for example be analysed during an investigation into sexual assault. Digital forensics can also be used to access volatile data of the kind normally encountered when investigating computer networks.

Together with a timestamp and in some cases geo-location, data from a device could corroborate or challenge any defence offered by a suspect. Figure 1 shows an example of how mobile phone data was used in an investigation conducted with Dutch authorities. Time stamp evidence is discussed further in Chapter 8.

Figure 1 Using mobile phone data that included a timestamp

Other sources of evidence include router and modem logs, together with any logs kept by the ISP. This form of evidence can corroborate when an internet connection was made and possibly to what location.

The increasing availability of Cloud-based data services such as DropBox (2007) and iCloud (Apple 2011) means that not all the relevant data may be held at the location being searched. Although a Court Order may be issued to secure this online data, timing is crucial as the subject of the investigation may promptly arrange for a third-party to erase the data remotely. The challenge to digital forensic investigation provided by Cloud storage is discussed further in Chapter 10. As well as Cloud-based data, digital forensic investigators are increasingly being asked to also examine the volatile data from the memory (RAM) of a powered on computer.

Having identified the sources of evidence to be examined, the next step is to secure a copy of this data in a 'forensic manner' and initially this typically concerns the preservation of evidence. Guidelines on evidence preservation have been produced both in the US (National Institute for Justice 2004) and

the UK (ACPO 2012) as well as other jurisdictions. However, inevitably the guidelines cannot cover every eventuality and hence there are times when knowledge and experience requires a judgment call on the part of the first responder. For example, in some cases the judgement will be to seize the computers concerned (including servers if necessary) whereas in other circumstances a decision will be made to image the hard drives and other forms of digital storage at the location with the hardware left intact in situ. This is particularly the case when data is being secured at a business address, when it is common practice to produce a forensic copy onsite to minimise any disruption to the business. A 1TB hard disk can be copied onsite in around 4 hours under certain conditions. This is preferable to taking the whole system away for around 24-48 hours for it to be processed and subsequently returned using additional entry requirements on the warrant. Whatever the decision, it is common practice in many countries to expect the first responder to make a careful note of the decision taken and the reasons for that decision.

Managing Suspects

The advice to be found in many national guidelines is that on arrival at the scene any suspects should be removed from the location and kept separately. Any 'advice' they provide should in general terms be ignored, since they could potentially be telling investigators to perform actions that lead to destruction of evidence. For example, if a suspect is asked for a password to log on to a live PC he/she may give the investigator an erroneous password which, when entered, causes the machine to run a script that destroys potential evidence stored on its hard drive. The suspect should be questioned when appropriate (in most cases once they are under caution at a police station) and asked for any passwords necessary to access any data seized. It may also be possible to obtain passwords from the scene on for example post-it notes (ACPO, 2012). Issues relating to passwords are covered in more detail in Chapter 3.

Is the Computer on or off?

When digital devices are encountered they may be either on or off, and is important that the correct actions are carried out in each case. This will depend on the exact situation; for example a PC that is in the process of downloading indecent images might well need to be left on by investigators, but a

PC involved in a distributed denial of service attack (DDoS) should probably be shut down as soon as possible. Note that it may be possible to retrieve plaintext encryption keys (Marshall, 2008) from machines left in a live state (but not running destructive processes). ACPO (2012) however provide some general rules to follow depending on the kind of device encountered and whether it is on or off.

For a PC that is switched off, under no circumstances should it be switched on since this would alter the machine's contents and could for example start up self-destruct scripts to wipe the its hard drive. The power cable from a desktop PC that appears to be switched off should be removed from the back of the PC, because it might only be in hibernate mode, with an uninterruptible power source supplied through the cable. The battery of a laptop should be removed without opening the lid as this can sometimes cause it to switch on (ACPO, 2012).

If the PC is switched on then the situation is more complex. A simple step that can be taken in most circumstances is to photograph the image on the screen of the PC. If no specialist advice is available and it is thought that no vital evidence will be lost by terminating any running processes then again the power cable should be removed (ACPO, 2012). However networks are commonly found to be involved in investigations. This will frequently be via the Internet, but other internal and external computer networks may also be present. An example of this would be an investigation involving the distribution of child abuse imagery via the Internet involving a number of networked PCs in a suspect's home or work environment. In these types of investigations "pulling the plug" may destroy vital information including any running processes, network connections, and any dynamically stored data in the RAM (ACPO, 2012). Dedicated software can be used to investigate live systems but it must be forensically sound and it will leave a "footprint" on running systems. Obviously this has to be taken into account in evidential terms (ACPO's second principle).

When securing volatile data, it is not enough to simply obtain a copy of the computer's RAM and analyse it. A computer's memory typically exists as a virtual block spanning both the physical RAM and 'paged' areas on the disk. Ideally both these elements should be examined together as a single entity. Furthermore, historical copies of RAM exist in hibernation files on laptops (from when the

laptop has gone to 'sleep') and crash dumps produced as a result of a Windows 'Blue Screen of Death' (BSoD).

It should also be a acknowledged that RAM analysis is still in its infancy and hence it is often necessary to corroborate findings from the RAM with other results achieved independently. For example, securing metadata (such as running processes and open ports or files) about the live system is useful means to compare with results obtained from RAM images. When working with live systems consideration should also be given to the order of volatility of data. A suggested approach (together with a study on the footprint of volatile data collection tools) has been suggested (Sutherland et al 2008)[2]. Greater detail (including suggested tools) has been provided in a malware analysis context (Malin et al, 2008)[3].

Preserving the evidence

Preservation of digital evidence typically involves the creation of a forensic copy (or 'image') of the evidence. This copy is then much more transportable and readily copied to produce working copies. At all times it is normally considered essential that any change to the original evidence is kept to a minimum. Under certain circumstances (eg: volatile data acquisition, see below) changing the original evidence is unavoidable; it is necessary to perform an action that will make a change to the original data. In keeping with ACPO guidelines and similar principles in other jurisdictions, when such actions are performed, their expected impact and the reasons for the actions are often expected to be recorded.

Many professional commentators suggest that the more documentation of the scene and the of investigators' activities the better: at a minimum the scene should be sketched, photographed and if possible videoed (Britz, 2004).

---

[2] Sutherland *et al*, *Acquiring volatile operating system data tools and techniques*, ACM SIGOPS Operating Systems Review, 2008

[3] Malin *et al*, *Malware forensics: investigating and analyzing malicious code*, Syngress Publishing, 2008

Copying, imaging and write-blocking non-volatile data

In many countries (but not all) standard practice is to make a 'copy' of seized data for analysis, with the general proviso that the copied data must be exactly the same as the original data. So for example to copy a hard drive, a simple tool such as Windows Explorer cannot be used as this only *appears* to make exact copies. Certain parts of the hard drive (such as files deleted and emptied from the Recycle Bin) are not generally retrievable by tools such as Windows Explorer and so will not be automatically copied. Instead, a specialist tool (often a combination of hardware and software) that performs a bit by bit copy is required; this creates what is known as an 'image' (Sammes and Jenkinson, 2007).

The capture of data on hard disks can take hours to complete. This may not always be a problem, but there is a finite amount of time a suspect can be held prior to a charging decision being made. Alternatively, it may be that the data capture is taking place under warrant at a business premises - again there is again a limited time that a warrant may allow forensic practitioners to remain on-site. Under both these circumstances, it is imperative that the forensic data capture is completed as quickly as possible.

An early action that a forensic practitioner is likely to take is to check the 'clock-time' on the PC whose hard drive is to be copied. All PCs have a BIOS clock on the motherboard, which many applications (some however will use an 'internet time' instead) running through the operating system will use to determine the date and time. Crucially, the BIOS clock cannot be assumed to be the correct date and time, and the difference with reality will need to be determined and recorded (see chapter 8 for further details).

For rapid data capture (also known as 'imaging'), hardware based solutions are preferred as these can currently provide data transfer rates of up to 7GB per minute at best. This would mean that a 500GB disk could be copied in just over an hour. In practice, this is highly dependant on the disk being copied which can reduce this speed significantly. Examples of hardware solutions include the Forensic Dossier (Figure 2) and the older Forensic Talon (Figure 3) (Logicube 2011).

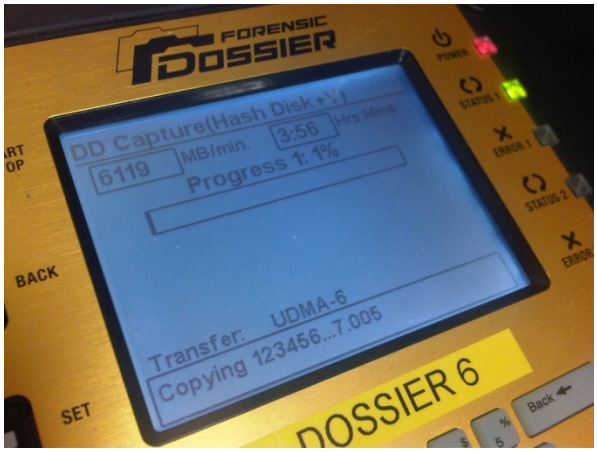

Figure 2

Figure 3 Data Imaging

Live Forensic Discs

A live forensic disc is a software-based imaging solution and consists of CD, DVD or USB. Some solutions provide a bootable operating system, typically Linux based. This allows a computer to be booted in a forensically sound manner, without the internal disk(s) being automatically mounted. Other solutions, such as the free tool FTK Imager for Windows (AccessData, 2010) are not bootable, but enable a first responder to capture live data from, say a server, that would not normally be taken offline. It is possible to create an image from a live and mounted disk, but the integrity of this copy is not as pure as an offline, forensic copy. This is because, files are subject to on-going changes by users or the operating system during the imaging process. Furthermore, it is not a repeatable process.

Some solutions, such as the Helix disc (e-fense 2011), provide both approaches on the same disc. This means the First Responder can decide upon arrival on the best approach to take and hence tools to use. Many First Responders will carry a few different versions and types of 'live forensic' discs in their toolkit. They can be used if there is a need to copy several disks simultaneously, or if the source hard disk does not work with their preferred solution.

Other examples of live forensic discs include Raptor (Forward Discovery 2011) and Paladin (Sumuri 2011). The Paladin disc also has a feature that allows the copy to be sent over a network to a network share on a remote computer. This can be useful if there are not enough USB ports on the source computer, or if the USB ports are faulty or restricted to the slower USB1.1 standard. A write blocker should be used when accessing (such as making a copy) the hard disk from an original exhibit held as 'Best' Evidence. Write blockers are hardware or software designed to prevent any writing to the target device. This ensures that the original evidence is kept pristine. It is necessary to take such precautions as even seemingly unobtrusive actions such as reading a hard drive may change its stored data (Knetzger & Muraski, 2008).

Once the forensic image has been captured a special number (called a 'hash') is calculated from both the source disk and the forensic image (see Chapter 8 on analysis of digital data). If both produce exactly the same number, then the copy is an exact copy of the original data.

Hashing

The authentication aspect of ACPO's first principle means that forensic practitioners must be able to show that any image that may subsequently be analysed is precisely the same as the original data (ACPO, 2012). A common method of demonstrating that a data image is an exact copy of the data initially seized is by the use of 'hashing' (Sammes and Jenkinson, 2007). A hash function is a mathematical algorithm (there are a number of such algorithms, two of the most popular are MD5 and SHA1) that takes an input and uses it to generate a much smaller "digest". The digest will always be the same for the same input, and any even slightly different inputs will generate very different digests (Stallings, 2010).

As an example of a hash, consider the contents of this paragraph preceding this sentence (ie "The authentication ... very different digests."). This would have an MD5 hash of

94696e913ca9198643a718276cd7d9df.

However the hash is very different if the same input has a single space added after the final fullstop (ie "The authentication ... very different digests. "). The hash becomes:

4924a5ecb7592543cc3dbaf87112ac1e.

Hashing has the additional useful property that hash functions are a one-way operation: the original input cannot be ascertained from a digest (Stallings, 2010). Note that although 'collisions' have been discovered in many hash functions these are so unlikely that in practice the system works as intended. The hash number generated by the calculation means that there is a 1 in 2^{128} chance of two different forensic images having the same hash value. Put another way, if over their professional career a forensic investigator produced over 340 340,282,366,920,938,463,463,374,607,431,768,211,456 forensic images, then the next forensic image produced would have the same hash as one of the proceeding images. This number can be recalculated at any time subsequent to the original data capture to confirm that neither the original disks nor the forensic copy have been changed.

Volatile data

In addition to the traditional hard disk imaging process, a more recent trend has emerged to acquire live (otherwise known as 'volatile') data from running systems. Computer hard disks contain a wealth of information for the forensic investigator, but some information may only exist in the Random Access Memory (RAM) of a computer whilst it is running. An analysis of RAM data can provide (AccessData 2009) information such as:

- a list of all the processes running and terminated on the computer;

- the path to where a program is located;
- command line arguments used;
- network connections (both idle and active);
- content from encrypted files that have been opened; and
- passwords entered by the user.

Network based data (called 'IP packets') containing IP addresses, and hardware identifying data known as Media Access Controller (or 'MAC') addresses have been recovered by Beverly et al (2011). This type of data can corroborate a hypothesis that two devices have communicated with each other over a network. (See Chapter 9 for further details).

In 2005 a challenge was set by the organisers of the conference DFRWS 2005 to develop a tool to acquire RAM from a running computer (DFRWS 2005). Two joint winners for the challenge were subsequently announced (Garner 2005), (Betz 2005). Ever since there has been an explosion of research in this area of data acquisition (Savoldi & Gubian 2008), (Simon & Slay 2009), (Walters 2006). (Kornblum 2007). One of the most versatile tools currently available to analyse RAM from Windows computers is Volatility (Volatile Systems 2007).

Referring back to the ACPO principles, there are two main considerations when acquiring volatile data. The first is the unavoidable fact that running a tool on a live computer system will change some of its memory (to allow the tool to be executed). Understanding the impact of this action, particularly how much memory is changed (also known as the 'footprint') is crucial to abiding by the second principle of the ACPO guidelines. The second consideration is that the memory of a live computer system is constantly undergoing change as a normal part of its operation. Consequently, current techniques to capture memory are unable to obtain a 'snapshot' of memory, because it changes more quickly than it can be written to a file. Hargreaves (2009) observed that the output obtained is more akin to a 'smear'.

Volatile data is not only found in RAM. Data stored online in what is termed the 'Cloud' can also be considered as volatile. Although the data is accessible through the Internet, the data itself is physically

stored on a server somewhere in the world. For a server located in the UK a warrant to access the specified server hosting the data can be exercised to secure a forensic copy of the data. However, for criminal investigations it is unusual to identify a UK located server. ~~and~~ Such a server is typically located in a jurisdiction where there is little or no means to gain lawful access to it, let alone a mechanism to arrest or even convict an offender. Part of the problem is the 'chain of richness creation' problem, common to developing countries (Lovet 2009). In the domain of money laundering, for example, such criminal activity benefits the local economy, which tends to undermine any political will to address the issue.

In the civil investigation arena, physical access can be gained through the co-operation of the owners of the server. This might be part of an investigation they have initiated or as part of a due diligence exercise. However, it may be impractical or unacceptable for a server to be taken offline to carry out a forensic imaging process of the internal disks. Under these situations software such as FTK Imager (AccessData 2011) can be executed from a USB memory stick to create a forensic copy of selected files and/or folders. As discussed above, the second ACPO principle must be taken into account when evaluating the impact of this approach.

PDAs and Mobile phones at crime scenes

Any PDA encountered at a crime scene should be left switched off if it is already in that state. However if A PDA is found to be switched on then consideration should be given to its battery life; it should be placed on charge as soon as possible. This is because any loss of power or switching it off could result in a situation where a password is required to access it when it is switched back on again. The same is true for smartphones and mobile phones, however these have the added complexity that in order to follow ACPO's first principle ~~one~~, a phone that is WIFI-enabled must be shielded from mobile phone networks and wireless networks (ACPO, 2012). Indeed**,** rapid isolation of PDAs, mobile phones and tablets from networks (including mobile data networks) is important for a number of reasons, not least of which is the ability of some devices to be 'remotely wiped'.

Isolation of a device can be performed in a number of ways as shown in the table:

Isolation Method	Benefits	Drawbacks
Switch the phone or device off	Simple, cheap, immediate.	A PIN or password may be required to access the device when it is switched back on.
Place the device in a Faraday bag such bags allow no electromagnetic signals to enter.	Simple, relatively cheap, immediate.	Only suitable to transport the device since the phone will continuously try and connect to a network when placed in such a bag thus draining the battery. Switching the phone to "airplane mode" may avoid this but will alter data on the device.
Use of a jamming device	Stops any alteration of the device and requires no software or hardware access to the device.	Illegal in the UK and other jurisdictions and may interfere with other devices/networks nearby.
Use of a Faraday tent – similar to a Faraday bag but a larger temporary structure.	Portable and allows room for examination.	Relatively expensive and requires time for setup. Any power cables entering the tent need to be screened otherwise they will act as antennas.
Use of a Faraday room – similar to Faraday tent but at a fixed location and permanent.	The ideal form of examination takes place in such a room, since it allows dedicated equipment that is either too heavy or fragile to be used in the field. Devices can be charged within the room.	Expensive, requires a lot of upfront costs and planning and not portable.
"Access card" type SIM. This is copied from the original SIM and thus has matching subscriber information, but the details required to access the network are removed.	Prevents the phone connecting to the mobile phone network.	Requires removal of the original SIM, which normally means battery removal hence the phone switches off. Requires a machine that can create such SIMs. When the access SIM is inserted data will change on the phone.
Contact Network Service Provider to block subscriber account.		Slow: requires Network Service Provider (NSP) cooperation and may require warrants. May result in future voice mails not being saved.

Seizure and Packaging

The power to seize evidence after a PACE section 18 search is provided under section 19. When handling any electronic equipment care should be taken since electrostatic charge can damage it.

Also grease, oil and other substances can damage equipment or contaminate it which could result in items becoming inadmissible as evidence. Therefore electronic equipment should be carefully packaged, avoiding materials such as plastic which may generate electrostatic charge (Britz, 2004, Bryant et al. , 2013).