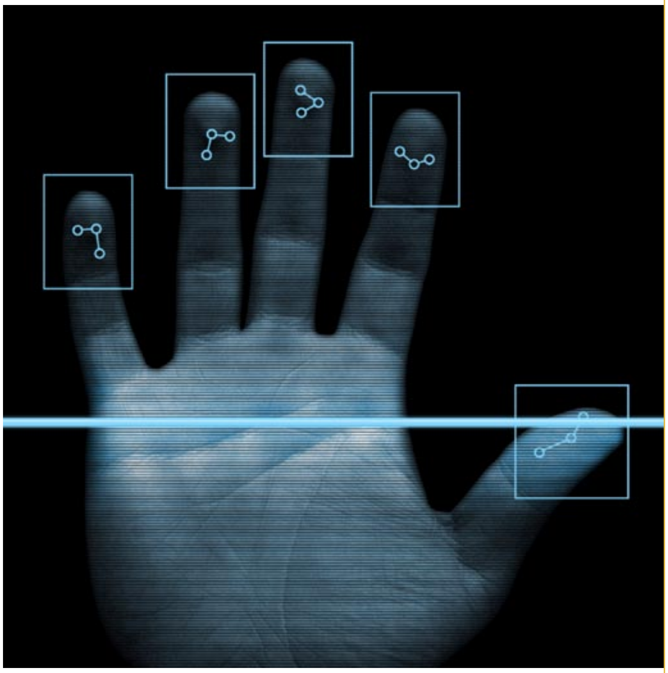
www.dns.co.uk

An introduction to:
Computer Forensics



about dns

dns is a leading provider of information security services in the UK. Our sole focus on information security provides us with the experience and expertise needed to provide security solutions to a wide range of public and private sector organisations throughout the UK.

Headquartered in Scotland, with offices in London and operating throughout the UK and Europe, **dns** provides security services across the full security lifecycle ranging from setting strategy and policy to design and delivery of secure infrastructure, service support and 24/7 management.

contact us

head office:
83 princes street,
edinburgh eh2 2er

london office:
16 st martin's le grand
london ec1a 4en

t: 0870 085 8555
f: 0870 085 8556
e: info@dns.co.uk

our services

consultancy

- information security governance
- regulatory compliance
- IT risk assessment
- CESG CLAS information assurance
- computer forensics

integration

- network security systems
- intrusion detection/prevention
- mobility and remote access
- identity and access management

testing

- IT security audit
- penetration testing
- web application security testing
- CESG CHECK testing

management

- managed firewall & vpn
- managed security monitoring
- managed email security
- managed vulnerability assessment
- security dashboard

dnsMSS™

table of contents

1 introduction

The Internet, networks, e-commerce, home users, portable devices and automated systems present a range of opportunities for committing criminal activity, or activity unauthorised in the workplace. Computers and other devices are being used increasingly to commit, enable, or support unwanted activity perpetrated against individuals, organisations, or assets.

Computer forensics has become a vital tool in providing evidence in cases such as computer misuse and attacks against computer systems as well as more traditional crimes such as murder, money laundering, drugs, abuse and fraud.

The Police, Crown Prosecution Service and the Procurator Fiscal criminal justice officials are being inundated by the quantity of investigations and prosecutions that involve electronic evidence. Consequently, the services of computer forensic experts are besieged by the volume of cases being handled and quite often less-experienced personnel are drafted in. Internal Audit, IT Service Desk, HR, Legal Services and Information Security are normally the types of departments called in to provide support. Unfortunately, these are also the members of staff that corrupt the evidence due to a lack of knowledge and understanding of the basic principles.

This **dns** White Paper is the first in a series designed to assist those without detailed forensic knowledge to conduct their activities appropriately prior to the provision of specialist **dns** services.

This guide is intended for use by those who have the responsibility for protecting an electronic incident or crime scene and for the recognition, collection, and preservation of electronic evidence. It covers the most common situations encountered with electronic evidence.

Without having the necessary skills and training, no one should attempt to explore the contents or recover data from a computer (e.g. do not touch the keyboard or click the mouse) or other electronic storage device other than to record what is visible on its display or to place in an evidence bag.

Note: Those handling such evidence should use caution when seizing electronic devices. The improper access of data stored in electronic devices may violate provisions of certain laws, including the Computer Misuse Act, and additional legal processes may be necessary. Please consult your legal representative before accessing stored data on a device.

this document will help you to:

- assess resources
- develop procedures
- assign roles and tasks
- consider staff safety
- identify equipment and supplies to bring to the scene

This paper is not intended to create definitive guidance and may not be relied upon in a Court of Law as a means of proving adherence to best practice. It is intended as a guide only. We encourage you to read the ACPO guidance. **dns** accepts no liability for errors or omissions.

2 computer forensics

Computer forensics is the generic name that we use for the analysis and reporting on our findings from the forensic analysis of all computer or digital-related media. This not only includes PC/Laptop or Server hard drives but also other storage devices such as USB drives, MP3 players, memory cards, SIMS and data gathered via network analysis.

All types of operating systems can be analysed, from DOS and Microsoft Windows-based, through to MAC, UNIX variants, and those utilising more obscure systems. If the data is stored electronically, then it can probably be forensically analysed.

common computer forensics cases include:

- drug dealing
- internet misuse
- pornography in the workplace
- rape
- illegal downloads
- IP theft
- paedophilia
- murder
- virus/malware infection
- fraud
- email analysis
- data recovery
- contract negotiations
- e-discovery
- peer-peer activities
- spyware analysis
- spoofed and threatening emails
- document tracking

The approach to securing evidence is vital. When dealing with electronic evidence, general forensic and procedural principles should be applied:

- actions taken to secure and collect evidence should not change that evidence.
- persons conducting examination of evidence should be trained for the purpose.
- activity relating to the seizure, examination, storage, or transfer of evidence should be fully documented, preserved, and available for review.
- evidence should be appropriately protected.

3 electronic devices: type and potential evidence

Electronic evidence can be found in many types of electronic devices, many of these found in most homes and offices. This chapter identifies a wide variety of the types of electronic devices commonly encountered, provides a general description of each type of device, and describes its common uses. In addition, it presents the potential evidence that may be found in each component.

Many electronic devices contain memory that requires continuous power to maintain the information, such as a battery or AC power. Data can be easily lost by unplugging the power source or allowing the battery to discharge. (Note: After determining the mode of collection, collect and store the power supply adaptor, cradle or cable, if present, with the recovered device - some devices may need to have this power source maintained.)

3.1 computer systems

description: A computer system typically consists of a base unit, sometimes called a central processing unit (CPU), data storage devices, a monitor, keyboard, and mouse. It may be a standalone or it may be connected to a network. There are many types of computer systems such as laptops, desktops, tower systems, modular rack-mounted systems, minicomputers, and mainframe computers. Additional components include modems, printers, scanners, wireless adapters, docking stations, and external data storage devices. For example, a desktop is a computer system consisting of a case, motherboard, CPU, and data storage, with an external keyboard and mouse.
primary uses: For all types of computing functions and information storage, including word processing, calculations, communications, Internet access, office applications, business applications, email, gaming and graphics.
potential evidence: Evidence is most commonly found in files that are stored on hard drives and storage devices and media. Examples are:

user-created files

User-created files may contain important evidence of relevant activity such as address books and database files that may prove certain associations, still or moving pictures that may be evidence of paedophile activity, and evidence of communications between parties such as by email or letter. Also, financial details may often be found in spreadsheets. Examples of user-created files:

- address books
- email files
- audio/video files
- image/graphics files
- calendars
- internet bookmarks/favourites
- database files
- spreadsheet files
- documents or text files

user-protected files

Users have the opportunity to hide evidence in a variety of forms. For example, they may encrypt or password-protect data that is important to them. They may also hide files on a hard disk or within other files or deliberately hide incriminating evidence files under an innocuous name.

- compressed files
- misnamed/renamed files
- encrypted files
- password-protected files

- hidden files
- steganography

Evidence can also be found in files and other data areas created as a routine function of the various types of computer operating systems. In many cases, the user is not aware that data is being written to these areas or files. Passwords, Internet activity, deleted files and temporary backup files are examples of data that can often be recovered and examined.

Note: There are components of files that may have evidentiary value including the date and time of creation, modification, deletion, access, user name or identification, and file attributes. Even turning the system on can modify some of this information. For example, the last time that a PC was booted or shutdown may be important.

computer-created files

- backup files
- log files
- configuration files
- printer spool files
- cookies
- swap files
- hidden files
- system files
- history files
- temporary files
- link files
- event logs

other data areas

- bad clusters
- other partitions
- computer date, time, and password
- reserved areas
- deleted files
- slack space
- free space
- software registration information
- hidden partitions
- system areas
- lost clusters
- unallocated space
- metadata
- boot records

3.2 components

3.2.1 central processing units (CPUs)

description: Often called the 'chip', it is a microprocessor located inside the computer. The microprocessor is located in the main computer box on a printed circuit board with other electronic components.

primary uses: Performs all arithmetic and logical functions in the computer. It controls the operation of the computer.

potential evidence: The device itself may be evidence of component theft, counterfeiting, or remarking.

3.2.2 memory

description: Removable circuit board(s) inside the computer. Information stored here is usually not retained when the computer is powered down.
primary uses: Stores user's programs and data while computer is in operation.
potential evidence: The device itself may be evidence of component theft, counterfeiting, or remarking. A large amount of evidence may be stored in memory (RAM) when the computer is powered up. This is lost when the machine is switched off.

3.2.3 access control devices - smart cards, dongles, biometric scanners

description: A smart card is a small hand-held device that contains a microprocessor that is capable of storing a monetary value, encryption key or authentication details (password), digital certificate, or other information. A dongle is a small device that plugs into a computer port that contains types of information similar to information on a smart card. A biometric scanner is a device connected to a computer system that recognizes physical characteristics of an individual (e.g., fingerprint, voice, hand, retina).
primary uses: Provides access control to computers or programs or functions as an encryption key.
potential evidence: Identification/authentication information of the card and the user, level of access, configurations, permissions, and the device itself.

3.2.4 digital cameras

description: Camera, digital recording device for images and video, with related storage media and conversion hardware capable of transferring images and video to computer media.
primary uses: Digital cameras capture images and/or video in a digital format that is easily transferred to computer storage media for viewing and/or editing.

potential evidence:

- images
- time and date stamps
- removable cartridges
- memory card
- video
- sound

3.2.5 hard drives

description: A sealed box containing rigid platters (disks) coated with a substance capable of storing data magnetically. Can be encountered in the case of a PC or laptop as well as externally in a standalone case.
primary uses: Storage of information such as computer programs, text, pictures, video, multimedia files etc.
potential evidence: See computer systems.

3.2.6 answering machines

description: An electronic device that is part of a telephone or connected between a telephone and a landline connection. Some models use magnetic tapes, while others use an electronic (digital) recording system.
primary uses: Records voice messages from callers when the called party is unavailable or chooses not to answer a telephone call. Usually plays a message from the called party before recording the message.
potential evidence: Answering machines can store voice messages and, in some cases, time and date information about when the message was left. They may also contain other voice recordings.

- caller identification information
- deleted messages
- last number called
- memo
- phone numbers and names
- tapes

Note: Since batteries have a limited life, data could be lost if they fail. Therefore, investigation personnel should ensure that a device powered by batteries is given the appropriate attention.

3.2.7 hand-held devices - personal digital assistants (PDAs), electronic organizers, iPAQ

description: A personal digital assistant (PDA) is a small device that can include computing, telephone/fax, paging, networking, wireless, Internet and other features. They are typically used as personal organisers and have almost the full functionality of a desktop computer system. Some do not contain disk drives, but may contain PC card slots that can hold a modem, hard drive, memory stick or other device. They usually include the ability to synchronise their data with other computer systems, most commonly by a connection in a cradle, or via Bluetooth or wireless. If a cradle is present, attempt to locate the associated hand-held device.
primary uses: Hand-held computing, storage, and communication devices capable of storage of information.
Note: Since batteries have a limited life, data could be lost if they fail. Therefore, investigation personnel should ensure that a device powered by batteries is given the appropriate attention.

3.2.8 memory cards

description: Removable electronic storage devices, which do not lose the information when power is removed from the card. It is possible to recover deleted data (e.g. erased images) from memory cards. Memory cards can store thousands of images in a small module. Used in a variety of devices, including computers, digital cameras, mobile phones, games consoles and PDAs. Examples are memory sticks, smart cards, flash memory, SD storage, and flash cards. There are many different types of these, usually FAT formatted.
primary uses: Provides additional, removable methods of storing and transporting information.
potential evidence: See potential evidence under computer systems.

3.2.9 modems

description: Modems, internal and external (analogue, DSL, ISDN, cable), wireless modems, PC cards.
primary uses: A modem is used to facilitate electronic communication by allowing the computer to access other computers (usually for Internet access) and/or networks via a telephone line, broadband, wireless, or other communications medium.
potential evidence: The device itself.

3.3 network components

3.3.1 local area network (LAN) card or network interface card (NIC)

Note: These components are indicative of a computer network.
description: Network cards, associated cables. Network cards can also be wireless.
primary uses: A LAN/NIC card is used to connect computers. Cards allow for the exchange of information and resource sharing.
potential evidence: The device itself, MAC (media access control) address.

3.3.2 routers, hubs, and switches

description: These electronic devices are used in networked computer systems. Routers, switches, and hubs provide a means of connecting different computers or networks. They can frequently be recognised by the presence of multiple cable connections.
primary uses: Equipment used to distribute and facilitate the distribution of data through networks.
potential evidence: The devices themselves. Also, for routers, configuration files.

3.3.3 servers

description: A server is a computer that provides some service for other computers connected to it via a network. Any computer, including a laptop, can be configured as a server. Generally, but not always, servers will have RAID drives and contain large amounts of storage.
primary uses: Provides shared resources such as email, file storage, web page services, data storage and print services for a network.
potential evidence: See computer systems.

3.3.4 network cables and connectors

description: Network cables can be different colours, thicknesses, and shapes and have different connectors, depending on the components they are connected to.
primary uses: Connects components of a computer network.
potential evidence: The devices themselves.

3.3.5 pagers

description: A hand-held, portable electronic device that can contain volatile evidence (telephone numbers, voice mail, email). Mobile telephones and personal digital assistants also can be used as paging devices.
primary uses: For sending and receiving electronic messages, numeric (telephone numbers, etc.) and alphanumeric (text, often including email).

potential evidence:

- address information
- text messages
- email
- voice messages
- telephone numbers

Note: Since batteries have a limited life, data could be lost if they fail.

3.3.6 printers

description: One of a variety of printing systems, including thermal, laser, inkjet, and impact, connected to the computer via a cable (serial, parallel, universal serial bus [USB]), firewire or accessed via an infrared port or wireless. Some printers contain a memory buffer, allowing them to receive and store multiple page documents while they are printing. Some models may also contain a hard drive or memory card. If they are printing, let them finish the print run.
primary uses: Print text, images, etc., from the computer to paper.
potential evidence: Printers may maintain usage logs, time and date information, and, if attached to a network, they may store network identity information. In addition, unique characteristics may allow for identification of a printer.

- documents
- hard drive/memory card
- ink cartridges
- network identity/information
- superimposed images on the roller
- time and date stamp
- user usage log

3.3.7 removable storage devices and media

description: Media used to store electrical, magnetic, or digital information (e.g. floppy disks, CDs, DVDs, cartridges, tape, USB drive).
primary uses: Portable devices that can store computer programs, text, pictures, video, multimedia files etc. New types of storage devices and media come on the market frequently and it is important to be able to recognise these.
potential evidence: See computer systems.

3.3.8 scanners

description: An optical device connected to a computer, which passes a document past a scanning device and sends it to the computer as a file.
primary uses: Converts documents, pictures etc. to electronic files, which can then be viewed, manipulated, or transmitted on a computer.
potential evidence: The device itself may be evidence. Having the capability to scan may help prove illegal activity. In addition, imperfections such as marks on the glass may allow for unique identification of a scanner used to process documents.

3.3.9 telephones
description: A handset either by itself (as with mobile telephones), or a remote base station (cordless), or connected directly to the landline system. Draws power from an internal battery, electrical plug-in, or directly from the telephone system.
primary uses: Two-way communication from one instrument to another, using land lines, radio transmission, cellular systems, or a combination. Phones are capable of storing information either on the phone itself, a SIM card, or a memory stick.
potential evidence: Many telephones can store names, phone numbers, and caller identification information. Additionally, many mobile telephones can store appointment information, receive electronic mail and Internet pages (similar to a PDA), and may act as a voice recorder, still or video camera.

- appointment calendars/information
- text messages
- password
- email
- caller identification information
- voice mail
- phone book
- memo/tasks
- electronic serial number
- internet usage

Note: Since batteries have a limited life, data could be lost if they fail.

3.3.10 game consoles
description: A hand-held (PSP) or static (PS2 / Xbox) gaming system powered via battery or DC.
primary uses: To play games. Some have wireless, and slots for memory cards and Internet capability
potential evidence: See computer systems.

3.3.11 miscellaneous electronic items
There are many additional types of electronic equipment that are too numerous to be listed that might be found at the scene of an incident. However, there are many non-traditional devices that can be an excellent source of investigative information and/or evidence. Examples are credit card skimmers, mobile phone cloners, caller ID boxes, dictation machines, Web TV or Sky boxes.

Fax machines, copiers, and multifunction machines may have internal storage devices and may contain information of evidentiary value.

REMINDER: The search of this type of evidence may require a search warrant.

4 investigative tools and equipment

principle: Special tools and equipment may be required to collect electronic evidence. Experience has shown that advances in technology may dictate changes in the tools and equipment required.
policy: There should be access to the tools and equipment necessary to document, disconnect, remove, package, and transport electronic evidence.

procedure: Preparations should be made to acquire the equipment required to collect electronic evidence. The needed tools and equipment are dictated by each aspect of the process: documentation, collection, packaging, and transportation.

Departments should have general crime scene processing tools (e.g., cameras, notepads, sketchpads, evidence forms, crime scene tape, markers). The following are additional items that may be useful at an electronic crime scene:

documentation tools

- cable tags
- indelible felt tip markers
- stick-on labels
- stationery

disassembly and removal tools

A variety of nonmagnetic sizes and types of:

- flat-blade and philips-type screwdrivers
- hex-nut drivers
- needle-nose and standard pliers
- secure-bit drivers
- small tweezers
- specialized screwdrivers (manufacturer-specific, e.g. hp, macintosh)
- wire cutters

package and transport supplies

- antistatic bags
- cable ties
- evidence tape
- sturdy boxes of various sizes
- used diskette (for transportation)
- antistatic bubble wrap
- evidence bags of various sizes
- packing materials
- parcel tape
- a means of secure transport

other items

Items that also should be included within a department's tool kit are:

- gloves
- digital camera
- large elastic bands
- list of useful telephone numbers
- mobile phone
- write blocker
- sim card reader
- magnifying glass
- blank paper
- seizure disk
- small torch
- unused floppy diskettes (3 ½ & 5 ¼)
- numerous and various cables etc.
- antistatic mat

5 securing and managing the scene

principle: Those first on the scene should take steps to ensure the safety of all persons at the scene and to protect the integrity of all evidence.
policy: All activities should be in compliance with your organisational policy and the Law.
procedure: After securing the scene and all persons on the scene, you should visually identify potential evidence, both conventional (physical) and electronic, and determine if fragile evidence exists. You should evaluate the scene and formulate a search plan.

5.1 secure and evaluate the scene

- follow your policy for securing the incident scene. This would include ensuring that all persons are removed from the immediate area from which evidence is to be collected. At this point in the investigation do not alter the condition of any electronic devices: **If it is off, leave it off. If it is on, leave it on.**
- protect volatile data physically and electronically. Volatile data may be found on pagers, PDAs, mobile phones, and other similar devices. You should always bear in mind that any device containing volatile data should be immediately secured, documented, and/or photographed.
- identify telephone lines attached to devices, such as modems. Document, label, and disconnect, each telephone line from the wall rather than the device, when possible. There may also be other communications lines present for LAN / Ethernet connections. Consult your forensic expert in these cases.

Keyboards, the mouse, diskettes, CDs, or other components may have fingerprints or other physical evidence that may require preservation. Chemicals used in processing prints can damage equipment and data therefore prints should be collected after electronic evidence recovery is complete.

5.2 conduct preliminary interviews

Identify all persons (witnesses, subjects, or others) at the scene and record their location at time of entry and subsequent movements.

Consistent with your organisational policy and PACE, obtain from these individuals information such as:

- owners and/or users of electronic devices or computers found at the scene, as well as passwords (see below), user names, and ISP
- passwords. Any passwords required to access the system, software, or data. (An individual may have multiple passwords e.g. BIOS, system login, network or ISP, applications, crypto, email, access token)
- purpose of the system
- any unique security schemes or destructive devices
- any offsite or removable data storage
- any documentation explaining the hardware or software installed on the system

6 documenting the incident

principle: Documentation of the scene creates a permanent historical record of the scene. Documentation is an ongoing process throughout the investigation and it is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence.
policy: Documentation of the scene should be created and maintained in compliance with your organisational policy and ACPO guidance.
procedure: The scene should be documented in detail.

initial documentation of the physical scene:

- observe and document the physical scene, such as the position of the mouse and the location of components relative to each other (e.g. a mouse on the left side of the computer may indicate a left-handed user).
- document the condition and location of the computer system, including power status of the computer (on, off, or in sleep mode). Most computers have status lights that indicate if the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, that may also indicate that it is on or was recently turned off.
- identify and document related electronic components that will not be seized.
- photograph the entire scene. The complete room should be recorded with 360° of coverage, if possible.
- photograph the front of the computer as well as the screen and other components. Also take written notes on what appears on the monitor screen.

Note: Movement of a computer system while the system is running may cause changes to system data. The system should not be moved until it has been safely powered down or switched off.

7 collecting the evidence

The search for and collection of evidence at an electronic incident scene may require a search warrant.

principle: Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidential value. This relates not just to the integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence therefore require special collection, packaging, and transportation. Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.
policy: Electronic evidence should be collected according to your organizational guidelines. In the absence of guidelines outlining procedures for electronic evidence collection, the following procedures are recommended.

Note: Prior to collection of evidence, it is assumed that locating and documenting has been done as previously described. Appreciate that other types of evidence such as DNA, or fingerprints may exist.

7.1 non-electronic evidence

Recovery of non-electronic evidence can be crucial in the investigation of cybercrime. Proper care should be taken to ensure that such evidence is recovered and preserved. Items relevant to subsequent examination of electronic evidence may exist in other forms (e.g. written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, literature, or computer printouts, and photographs) and should be secured and preserved for future analysis. These items frequently are in close proximity to the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with your policies.

7.2 stand alone and laptop computer evidence

Multiple computers may indicate a network. Likewise, computers located at businesses are often networked. In these situations, specialised knowledge about the system is often required to effectively recover evidence and reduce your liability. When networks are encountered, contact your computer forensic expert for assistance.

A ‘stand-alone’ personal computer is a computer not connected to a network or other computer. These may be desktop machines or laptops.

Laptops incorporate a computer, monitor, keyboard, and mouse into a single portable unit. Laptops differ from other computers in that they can be powered by electricity or a battery source therefore they require the removal of the battery in addition to stand-alone power-down procedures.

If the computer is on, document existing conditions and contact your expert. If an expert is not available, continue with the following procedure:

After securing the scene, read all steps below before taking any action (or evidentiary integrity may be lost).

a. Record in notes all actions you take and any changes that you observe in the monitor, computer, printer, or other peripherals that result from your actions.

b. Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

condition 1: Monitor is on and last activity and/or desktop is visible.

1. Photograph screen and record information displayed.
2. Proceed to step c).

condition 2: Monitor is on and screen is blank (sleep mode) or screensaver is visible.

1. Move the mouse slightly (without pushing buttons). The screen should change and show last activity or request a password.
2. If mouse movement does not cause a change in the screen **DO NOT perform any other keystrokes or mouse operations.**
3. Photograph the screen and record the information displayed.
4. Proceed to step c).

condition 3: Monitor is off.

1. Make a note of ‘off’ status.
2. Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.

c) Regardless of the power state of the computer (on, off, or sleep mode), remove the power cable from the computer **NOT** from the wall socket. If dealing with a laptop, in addition to removing the power cord, remove the battery. The battery is removed to prevent any power to the system. Some laptops have a second battery in the multipurpose bay instead of a floppy or CD drive. Check for this and remove that battery as well.

- check for outside connectivity (e.g. telephone modem, cable, ISDN, DSL, wireless). If a telephone connection is present, attempt to identify the telephone number.
- to avoid damage to potential evidence, remove any floppy diskettes that are present, package the diskette separately, and label the package. If available, insert either a forensic boot disk or a blank floppy disk. Do **NOT** remove CDs or touch the CD drive.
- place tape over all the drive slots and over the power connector.
- record make, model, and serial number.
- photograph and sketch the connections of the computer and corresponding cables.
- label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly at a later time. Label unused connection ports as ‘unused’. Identify laptop computer docking stations in an effort to identify other storage media.
- record or log evidence according to your procedures.
- if transport is required, package the components carefully.

7.3 computers in a complex environment

Company environments frequently have multiple computers connected to each other, to a central server, or both. Securing and processing a scene where the computer systems are networked poses special problems, as improper shutdown may destroy data or disrupt the business. This can result in loss of evidence and potential liability. When investigating activity in a known business environment, if possible, the presence of a computer network should be planned for in advance and appropriate expert assistance obtained. It should be noted that computer networks can also be found in a home environment and the same concerns exist.

The possibility of various operating systems and complex hardware configurations requiring different shutdown procedures make the processing of a network incident scene quite complicated. It is important that computer networks can be recognised and identified, so that expert assistance can be obtained.

Indications that a computer network may be present include:
The presence of multiple computer systems.

- the presence of cables and connectors, running between computers or central devices such as hubs
- information provided by individuals at the scene
- the presence of network components
- a wireless PCMCIA / USB device, or an access point or aerial

7.4 other electronic and peripheral evidence

The electronic devices such as the ones shown below may contain potential evidence associated with certain activity. Unless an emergency exists, the device should not be operated. Should it be necessary to access information from the device, all actions associated with the manipulation of the device should be documented. Many of the items below may contain data that could be lost if not handled properly.

- dictation machine
- cables
- mobile telephones
- photocopier
- digital cameras (still and video)
- games consoles
- external drives
- flash memory cards
- GPS devices e.g. TomTom
- pagers
- printers (if active, allow to complete printing)
- scanners
- telephones
- answering machines
- caller ID devices
- other hardware
- PDA device
- removable media, USB devices
- CD jukeboxes
- fax machines
- floppies, diskettes, CDROM, DVD
- PCMCIA cards
- MP3 Players
- dongle or other hardware protection devices (keys) for software
- smart cards/secure ID tokens
- wireless access point

Note: When seizing removable media, ensure that you take the associated device that created the media (e.g. tape drive, cartridge drives such as Zip, Jaz).

8 packaging, transporting and storage

principle: Actions taken should not add, modify, or destroy data stored on a computer or other media. Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and magnetic sources. Therefore, special care should be taken when packaging, transporting, and storing electronic evidence. To maintain chain of custody of electronic evidence, document its packaging, transportation, and storage.
policy: Ensure that proper procedures are followed for packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.

packaging procedure:

a. Ensure that all collected electronic evidence is properly documented, labelled, and recorded before packaging.

b. Pack magnetic media in antistatic packaging (antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags.

c. Avoid folding, bending, or scratching computer media such as diskettes, CDROMs, DVDs, and tapes.

d. Ensure that all containers used to hold evidence are properly labelled.

Note: If multiple computer systems are collected, label each system so that it can be reassembled as found (e.g., CPU01-mouse, keyboard, monitor, base unit; CPU02-mouse, keyboard, monitor, base unit).

8.1 transportation procedure

a. Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.

b. Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.

c. Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the car floor and monitors placed on the seat with the screen down and secured by a seat belt.

d. Maintain the chain of custody on all evidence transported.

8.2 storage procedure

a. Ensure that evidence is documented in accordance with your policies.

b. Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.

Note: Be aware that potential evidence such as dates, times, and system configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail.

9 potential evidence by category of incident

The following outline should help investigators identify the common findings of a forensic review as they relate to specific categories. This may also help define the scope of the examination to be performed.

9.1 auction fraud (e.g. eBay)

- account data regarding online auction sites
- chat logs
- address books
- calendar
- accounting/book-keeping software and associated data files
- customer information/credit card data
- databases
- digital camera software
- email/notes/letters
- financial/asset records
- image files
- internet activity logs
- internet browser history/cache files
- online financial institution access software
- records/documents of ‘testimonials’
- telephone records

9.2 child abuse

- user-created directory and file names that classify images (lolita)
- date and time stamps
- digital camera software
- email/notes/letters
- games
- peer-peer software
- graphic editing and viewing software
- images
- internet activity logs
- movie files
- chat logs
- internet searches

9.3 computer/network intrusion

- address books
- configuration files
- email/notes/letters
- executable programs
- IDS logs
- internet activity logs
- IP address and user name
- IRC logs
- source code
- text files (user names and passwords)

9.4 murder/death investigation

- address books
- diaries
- email/notes/letters
- financial/asset records
- images
- internet activity logs
- legal documents and wills
- medical records
- telephone records
- other documents

9.5 domestic violence

- address books
- diaries
- email/notes/letters
- financial/asset records
- medical records
- telephone records

9.6 fraud (including online fraud)

- address books
- cheque, currency, and postal order images
- credit card skimmers
- online financial institution
- email/notes/letters
- spreadsheets
- financial/asset records
- calendar
- customer information/credit card data
- internet activity logs
- databases
- false financial transaction forms
- false identification.
- images of signatures

9.7 email threats/harassment/stalking

- address books
- diaries
- email/notes/letters
- financial/asset records
- images
- internet activity logs
- legal documents
- telephone records
- victim background search
- chat logs

9.8 gambling

- address books
- calendar
- customer database and player records
- customer information/credit card data
- electronic money
- email/notes/letters
- financial/asset records
- images of players
- internet activity logs
- online financial institution access software
- sports betting statistics
- spreadsheets

9.9 identity theft

- hardware and software tools
- backdrops for ID cards
- credit card generators
- credit card reader/writer
- digital cameras
- scanners
- identification templates
- birth certificates
- cheque guarantee cards
- digital photo images for photo ID
- driving licence
- electronic signatures
- internet activity at forgery sites
- emails and newsgroup postings
- online trading information
- online orders
- internet activity related to ID theft
- scanned signatures
- car insurance documents
- fictitious vehicle registrations
- cashiers' cheques
- counterfeit money
- credit card numbers
- travellers cheques

THE VIEWS AND OPINIONS OF THE AUTHOR DO NOT NECESSARILY REFLECT THOSE OF DNS LTD.

WITH RESPECT TO INFORMATION CONTAINED IN THIS DOCUMENT, NEITHER DNS LTD. NOR ANY OF ITS EMPLOYEES MAKE ANY WARRANTY, EXPRESS OR IMPLIED, OF FITNESS FOR A PARTICULAR PURPOSE.

NEITHER DNS LTD., NOR ANY OF ITS EMPLOYEES ASSUME ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, OR PROCESS DISCLOSED.

ACKNOWLEDGEMENT
THIS DOCUMENT IS BASED UPON ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS WRITTEN AND APPROVED BY THE TECHNICAL WORKING GROUP FOR ELECTRONIC CRIME SCENE INVESTIGATION, PUBLISHED IN JULY 2001. IT HAS BEEN UPDATED TO REFLECT CURRENT PRACTICES AND ANGLICISED TO A DEGREE BUT THE BODY AND FORMAT REMAINS AS ORIGINALLY WRITTEN.