International
Competition
Network

ANTI-CARTEL
ENFORCEMENT MANUAL

CARTEL WORKING GROUP

Subgroup 2: Enforcement Techniques

March 2010

Chapter 3
Digital Evidence Gathering

www.internationalcompetitionnetwork.org

CONTENTS

1 INTRODUCTION

In today's world of advancing technologies, more and more information is being generated, stored and distributed by electronic means. This requires many agencies to increase the use of digital evidence gathering as a frequent or standard tool in their fight against cartels. This Chapter on Digital Evidence Gathering aims to provide an overview of practices and procedures for digital evidence gathering of ICN member agencies.

The chapter is based on information collected from ICN members in November 2009 by means of a questionnaire to which 24 member agencies sent a reply.[1] The aim of the questionnaire was to update the information gathered four years ago for the first *Anti - Cartel Enforcement Manual*. The text therefore seeks to encompass the new information as well as instructive information from the previous version of the chapter. It has become apparent that agencies have strengthened their efforts in the sector of digital evidence gathering. These developments have made an update of this chapter necessary.

The Manual and this Chapter shall help to better understand the range of ICN member approaches to digital evidence gathering and to identify good practices and procedures with respect to digital evidence gathering and the use of digital evidence in the context of the investigation, adjudication or prosecution of cartels. In order to make this a comprehensive and practical work product both member agencies and other stakeholders such as non-governmental advisors were invited to submit their comments.

As in the previous chapters, best efforts were made to reflect the input of all the agencies. However, where there is a reference in the Chapter to the number of agencies that engage in any particular practice or procedure, it should be recognized that this may not be a precise reflection of the experience of all the responding agencies. In some instances, usually due to either confidentiality concerns or to a lack of practical experience, some responding agencies indicated they could not provide information. In addition, some agencies provided additional information that was not requested by the questionnaire. Where possible, this additional information is included in the Chapter.

Even though there may have been rapid technical developments since the Chapter was first written, many observations made in the first version still hold true. Although some of these statements were not necessarily or explicitly reiterated by the respondents to the latest questionnaire, they are still included in order to give an extensive overview of the subject.

This Chapter should be read in conjunction with the Chapter on Searches, Raids and Inspections, which provides an overview of the general approach of member agencies to searches, raids and inspections and sets out some good practices.

The *Anti - Cartel Enforcement Manual* is a work in progress. This Chapter reflects the current status of digital evidence gathering at the different member agencies. It is in no way meant to be static or all-inclusive. As technology, software and hardware change continuously, the definitions used and the methods for collecting, analyzing and ensuring the admissibility of digital evidence will also be subject to change.

[1] The responding agencies are listed in Appendix 2.

2 DEFINITIONS AND QUALIFICATIONS

The definitions mentioned below have been used for the purpose of the questionnaire sent out to the ICN members and do not necessarily represent the definitions used by the different agencies. They are meant as points of reference in order to have a common understanding of digital evidence gathering among agencies for the purposes of this Chapter.

2.1 Defined Terms

- **Computer Forensics** is the use of specialized techniques for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information. Computer forensics comes into play when a case involves issues relating to the reconstruction of computer system usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer Forensics requires specialized expertise that generally goes beyond normal data collection and preservation techniques available to end-users or system support personnel.
- **Digital information** is all information in digital form and can be divided into the content itself (of a text document, a drawing or photo, a database, etc.), and the information about this content, the so called metadata (filenames, pathnames, the date and time that a document has been created or edited or an e-mail has been sent, received or opened, the creator/ sender of a document or e-mail, etc.). It is often not possible to handle digital information without acquiring knowledge of at least some of this metadata.
- **Digital evidence** is all digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the storage media (data carrier), the tapping or monitoring of network traffic, or the making of digital copies (forensic images, file copies, etc), of the data held. Although hard copy print outs of digital information are not digital evidence in the strict sense of this definition, it is considered a starting point for applying digital evidence gathering in the future.
- **Forensics** is the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for a court of law or other legal context.
- **Chain of custody** is the record of the custodial history of the evidence.
- **Chain of evidence** or authentication is the record of the collection, processing and analysis of the digital evidence. It proves that the presented evidence is unequivocally derived from the acquired digital information.
- A **data carrier** is any device that contains or transports digital information and includes a physical hard drive, a floppy disk, Personal Digital Assistants (PDAs), Universal Serial Bus devices (USBs), a SIM-card from a cell phone, a flash memory stick/card, a network and a server, etc. This list is non-exhaustive.
- A **hash value** is a mathematical algorithm produced against digital information (a file, a physical disk, a logical disk) thereby creating a digital fingerprint for that information. It is by purpose a one-way algorithm and thus it is not possible to change digital evidence, without changing the corresponding hash values. In other words, if the hash value of a file has (not) changed, the file itself has (not) changed.
- A **forensic image** (sometimes called a forensic copy) is an exact bit-by-bit copy of a data carrier including slack, unallocated space and unused space. There are forensic tools available for making these images. Most tools produce information, like a hash value, to ensure the integrity of the image.

- **Live forensics** consists of seizing or analysing system information, memory contents and/or contents of data carriers from live systems (running). This extracts information from live memory (information which is lost when the computer is powered down).
- **Cloud computing** describes a new supplement, consumption and delivery model for IT services based on the Internet, and typically involves the provision of dynamically scalable and often virtualised resources as a service over the Internet. This comprises common business applications online which are accessed from a web browser, while the software and data are stored on servers in unknown locations on the Internet.

3 IMPORTANCE OF DIGITAL EVIDENCE GATHERING

3.1 The advantages of digital evidence gathering

In many jurisdictions, digital information gathered during searches, raids, or inspections, or obtained through compelled discovery, even if not decisive by itself, has contributed to proving competition infringements. Digital evidence gathering is becoming an increasingly powerful tool for agencies in their fight against cartels. It can be used individually or alongside more traditional methods of evidence gathering. Agencies have indicated that the collection and the review of digital evidence have become a standard and regular practice in cartel investigations. As more companies become aware of the forensic techniques used by competition authorities it is important to continue to develop digital evidence gathering techniques. This will ensure that companies will not be able to anticipate all methods which will be used by competition authorities during an investigation.

Digital Evidence may be used as key evidence, however some authorities stated that it could serve as a complement to other types of evidence. Furthermore, digital evidence may help in the course of the investigation phase to prepare the next steps.

The use of digital evidence gathering in cartel investigations has some clear advantages:

3.2 Some information has not nor ever will exist on paper

Developments in technology influence the way in which companies create and store digital information. Companies rely to a lesser extent on hard-copy documents. Some hard-copy documents located at a search, raid or inspection site, or obtained through compelled discovery can be a hard copy print-out of digital information, while other information may never appear in paper format. This information will not be obtained when gathering evidence in more traditional ways.

3.3 Some information in hard-copy was destroyed

Companies under investigation for competition infringements are increasingly looking for ways to avoid agencies finding evidence that may contribute to proving these infringements. Destroying hard-copy documents is an easy way of hindering or obstructing the investigation. Using digital evidence gathering for locating evidence does not in any way rule out the possibility of obstruction of the investigation. It does however provide the possibility of recovering deleted or destroyed evidence. In more traditional ways of gathering evidence, this would not be possible.

3.4 Hard-copy information is limited to the content

Information or evidence that can be derived from a hard-copy document is limited to the content of the document. Digital files or programs on the other hand also contain metadata or data about the digital information which can give access to a new source of information. It can provide information about the origin, size and format of the digital information, including the author of a file and the date when it was created, last altered, accessed or deleted. It may also give detailed information about the revisions of a document. Information can also be obtained concerning the exchange of information, the identity of the sender and receiver of the digital information and what actions individuals have undertaken with this information.

Digital evidence gathering has in some jurisdictions contributed to proving competition infringements. It is clear that digital evidence gathering is becoming increasingly important. Nevertheless, it is still an additional method and will not replace more traditional ways of evidence gathering in the short term.

4 LEGAL AUTHORITY

92% of the responding agencies indicated that they have the legal authority to gather digital evidence and 83% of the responding agencies have used their powers. Some agencies require a search warrant or court order, while other agencies may have the authority to order these measures themselves.

Most agencies indicated that in their national law there is no explicit legal provision for digital evidence gathering. The legal basis for digital evidence gathering is derived from the interpretation of already existing provisions in national laws that permit the agencies to collect or seize documents.

Some examples:

- One agency reported that the legal basis for collecting digital evidence flows from the existing right of the agency to collect any documents – paper or digital – that are relevant to the investigation.
- One agency is entitled to examine the books and other records related to the business, irrespective of the medium on which they are stored, and to take or obtain in any form copies of or extracts from such books or records. This also covers digital evidence.
- One agency explained that the power for collecting digital evidence is not specifically stipulated in their national law. An object to be retained must be tangible, so digital information itself, which is intangible, may not be retained or seized, but the storage media in which digital information is recorded may be retained or seized.
- One agency has powers to obtain information, documents and evidence relating to a matter that constitutes, or may constitute an infringement. This agency uses a broad definition of 'documents' that include "...a disc, tape, paper or other device from which sounds or messages are capable of being reproduced". This also encompasses digital evidence.
- One agency is entitled to order the inspection of business data and documents, and to make copies of the data and documents. Data recorded by electronic means falls within the scope of the definition.
- One agency explained that its national law defines 'document', as including any information recorded or stored by means of any tape recorder, computer or other device and any material subsequently derived from information so recorded or stored.
- One agency reported that two laws give explicit directions for digital information gathering. The new amendments of the competition law and the background procedural law are more explicit and provide detailed rules for digital searching and forensic image making. The rules also determine the procedural steps concerning legal privilege.

Other agencies stated that the legal basis for collecting digital evidence is explicitly put down in the relevant laws.

Some examples:

- One agency responded that there was an explicit legal basis for collecting digital evidence. The act defines "records" to include "...photograph, film, microfilm, sound recording, videotape, machine readable record, and any other documentary material, regardless of physical form or characteristics, and any copy or portion thereof".
- One agency reported that according to the law the inspecting persons are authorised to request "files, books, all kinds of documents and data carriers related to the subject of the inspection as well as extracts thereof".

5 MAIN DISTINCTIONS IN DIGITAL EVIDENCE GATHERING

There are two main practices used by agencies to gather digital evidence: searches, raids and inspections on the one hand, and compelled discovery on the other hand. A majority of the responding agencies use searches, raids and inspections as their primary tool; only some use both searches, raids and inspections, and compelled discovery.

5.1 Searches, Raids and Inspections

Digital evidence gathering by means of a search, raid or inspection can be carried out in different ways. Some agencies are allowed to seize digital information. Others can copy or make forensic images of digital information. In most cases this information is collected on-site, but analyzed at a later time. This generally takes place at the offices of the agency.

Of the replies to the questionnaire, the vast majority of agencies use (or would be able to use) searches, raids or inspections as the primary tool for collecting digital information. Not all authorities have actually used their powers to perform digital evidence gathering during searches, raids or inspections.

- One agency “may inspect, give an order to submit, or retain storage media in which digital information is recorded, subject to the consent of the company under investigation. Investigators may then operate personal computers and view the digital information in storage media to determine whether it contains digital evidence relevant to the case, subject to the consent of the administrator of such PCs.”
- One agency is “authorized to collect digital evidence by using inspections, or later at anytime during the investigation. The agency recognises that more results are made during inspections, but sometimes after having discovered new leads, it may be worthwhile to collect new information.”
- One agency is authorized to conduct an inspection. The agency makes print-outs of digital documents.

5.2 Compelled Discovery

Compelled discovery, whether by subpoena, order for production or request for information, is used to compel companies or individuals to produce any requested documents or records– whether paper or digital – that are relevant to the investigation. An agency may compel a company or individual to preserve all potentially responsive digital evidence. In this case, it is the company or individual and not the agency that performs a thorough search for all responsive evidence and produces the evidence in an acceptable format. It is important to learn about the computer systems and the efforts made by the company to preserve digital information. The search methodology used by the company is also an important issue.

Several agencies reported use of or ability to use compelled discovery for digital evidence gathering in addition to searches, raids or inspections.

- A number of agencies make written requests (sometimes called statutory notices) for digital evidence. Companies can be requested to produce information in form of printouts, CD-ROM/DVD, floppy discs or other portable media where this is considered to be the most appropriate medium.
- One agency reported to have broad authority to conduct criminal investigations, including issuing document subpoenas to companies and individuals suspected of engaging in anticompetitive activity. These subpoenas compel companies to produce to the government any requested documents – whether paper or digital – that are relevant to the grand jury investigation. The agency collects digital evidence primarily through the use of document subpoenas.
- Another agency reported collecting digital evidence by means of a Court order requiring an individual or companies to produce records, including records in digital form.

- One agency reported “to have powers to obtain information, documents and evidence relating to a matter that constitutes, or may constitute, a contravention of competition law. The agency may seek written answers to questions, require the production of documents and compel individuals to attend interviews and answer questions about possible infringements.”
- One agency stated that “it can issue or obtain, in any form, copies or excerpts from documents, account books, financial, accounting and commercial documents or other evidence related to the business of the company or the association of companies.”

6 RESOURCES FOR DIGITAL EVIDENCE GATHERING

6.1 Staff

Digital evidence gathering as an investigative tool requires special skills and expertise that go beyond normal information collection and preservation techniques. Gathering digital evidence from electronic devices means that staff must be up-to-date with the latest technological developments and techniques. Therefore staff needs to put a lot of effort into training and study. Management must also be supportive by allocating time and financial resources to staff training.

6.2 The position of digital evidence gathering in the organisation

It is good practice to have a dedicated internal organisation or staff capacity to undertake digital evidence gathering.

58 % of all responding agencies have some dedicated internal organisation or staff capacity to undertake digital evidence gathering.

Only a few agencies have a specialised unit dealing with digital evidence gathering. The number of people working in these units varies. These units generally work in the collecting phase but they have a special role in the early processing phase, i.e., indexing or retrieval of the digital information. One agency has a specialised team dedicated to digital evidence gathering and have trained many further officers in this subject.

Some of the agencies that do not have a specialised unit have specialists working in their information technology (IT) department who dedicate part of their time to digital evidence gathering. These specialists also assist case teams during searches, raids or inspections, and analysis of digital evidence.

Other agencies that do not have a specialised unit have trained some of their officers in the basics of digital evidence gathering. These trained officers are used in the collecting phase and later on are also used in the processing and investigating phases. Even concerning the analyzing phase most agencies use officers who have received some specialised training (case handlers) with the support of the IT specialists. Working with the digital evidence gathered is thus generally a combined effort of IT specialists and case handlers at different stages of the case.

Outsourcing digital evidence gathering to private companies is a practice of a minority of the agencies. Outsourcing such an activity is generally subject to national procurement rules. This outsourcing concerns the retrieval of digital information and partially the processing preparation work, but hardly ever the analysis of the digital information.

Outsourcing digital evidence gathering to other public entities is a practice some agencies engage in frequently. This concerns not only the retrieval of digital information, but also the analysis of digital information, however in this phase usually the external party works together with the case handlers.

In all cases of outsourcing digital evidence gathering to private companies, the companies involved have to sign either a statement on confidentiality or a confidentiality agreement. In some cases there are also agreements restricting the companies from working for companies under investigation of the agency.

6.3 Officers and forensic specialists

It is good practice for officers and forensic specialists to work closely during all stages in the gathering of digital evidence.

When it comes to analysing digital information, there should be a close working relationship between the IT-staff / Forensic Analysts and the case handlers. This working relationship typically starts at the earliest possible moment in order to ensure that the relevant digital information is copied and prepared for analysis in the most effective way. At some agencies this working relationship starts at a later phase namely when the collection of digital information is settled.

In many jurisdictions the staff is not solely responsible for the collection of the digital information and certain agencies may rely exclusively on IT-experts, particularly in the case of IT forensic.

6.4 The training of staff

It is good practice to give special training to the agency's staff that collect and process digital evidence.

Almost all agencies practicing digital evidence gathering give their staff (forensic specialists or officers) some training. Forensic IT specialists are well-trained in utilization of the main Forensic IT software.

Officers may be provided with some training ranging from a basic course on digital evidence gathering to special training to copy and/or analyse digital information. Most agencies which involve officers in digital evidence gathering ensure that officers receive a course on the principles of digital evidence gathering. The main purpose appears to be to promote a better understanding and communication between the officers and the computer forensic specialists in or outside the agencies.

In some cases, training is provided by the suppliers of the software used when practising digital evidence gathering. In a number of other cases training is provided by other public agencies working in the field of criminal or administrative enforcement, such as the police, customs, tax police and the fraud office.

The International High Technology Crime Investigation Association Annual Training Conference also provides a venue for the gathering and sharing of information between international computer forensic specialists and provides non-vendor specific trainings. In order to maintain knowledge on developments, some agencies participate in knowledge-oriented networks of national enforcement agencies. For example, in 2009 the Italian Competition Authority promoted and realized a European project of specialized training, co-funded by the European Commission under the Program “Prevention of and Fight against Crime”. Twenty-three agencies in Europe have participated in this training project. This project has been articulated in three educational segments:

- “Basic / Intermediate training seminars in computer forensics”: all aspects of a forensic examination, which included a training course to achieve the Certified Computer Examiner (CCE).
- “Inspections other than with keyword searches in files”: aimed to present a more advanced view in the field, by focussing on the identification and gathering of digital evidence through the analysis of administrative organization and internal control processes.

- “DG COMP’s model in applying Forensic IT”: contributing to a better understanding of procedures and techniques followed by the EC officers and, as a result, to a more effective cooperation of national competition authorities providing investigatory assistance,

This project has strengthened the European network of Forensic IT experts, sharing techniques, methods and procedures, as well as experience.

Furthermore a number of agencies in Europe participate in the Annual European Forensic IT meeting. During this meeting experiences and best practices are exchanged between computer forensic specialists of the participating agencies. Both technical and legal experts take part in this conference.

6.5 Co-operation with other public agencies

It is good practice to describe the scope and nature of cooperation with other public agencies in a protocol.

33 % of the responding agencies have some kind of cooperation on digital evidence gathering with other public agencies. Whereas some agencies use other public agencies for the retrieval, copying and analysis of digital information, most agencies only let the public agency assist them when copying digital information.

7 ELEMENTS OF DIGITAL EVIDENCE GATHERING

7.1 Tools (Software and Hardware)

It is good practice to use tools that are thoroughly tested and generally accepted in the computer forensics field.

Almost all agencies use commercially available computer forensic tools for digital evidence gathering. The use of self-developed software is, in general, limited. While all agencies do not limit their searches to PCs and Laptops, but also examine CD-ROMs, DVDs and USB devices, a few agencies have noted that searching smart phones and cell phones may be restricted by national laws governing telecommunications.

Software[2] that may be used for gathering and analysing digital information includes:

- Boot Software – used to start a computer for imaging and / or analysis without making changes to the hard drive
- Computer Forensic Software – used for imaging and analysing digital information
- Forensic software write blockers – used to allow acquisition of digital information on a hard drive without changing and altering the contents
- Hash Authentication Software – used to validate that a copy of digital information is identical to the original information
- Analysis Software – used for analysing digital information or extracting digital information from cell phones and PDAs
- Bit stream imaging software – used to create an image of all areas of a data carrier. A bit stream image is an exact replica of each bit contained in the data carrier
- Intelligence Analysis Software – used to create a link chart, a time line and a theme line with computer graphical software
- Anti-Virus Software – used to protect the computers (of the party being investigated and the agency) from viruses
- General Application Software – used to create digital information
- Litigation Support Software – used to store, organise, analyse and retrieve digital information in preparation for court proceedings
- Backup Software – used to retrieve or produce a copy of digital information

Hardware[3] that may be used for gathering and analysing digital information includes:

- Search box – used to carry equipment to and from the premises
- Bridges – used to connect external hard drives to a laptop or computer to copy or analyse digital information
- Camera – used to take photographs at the premises

[2] Types of software and hardware are not necessarily mutually exclusive and may be used for multiple purposes

[3] Types of software and hardware are not necessarily mutually exclusive and may be used for multiple purposes.

- Cell phone Analysis Tools – used to read SIM cards
- Drive Copier – used to copy a master hard drive to a number of hard drives for forensic copies or disclosure
- Drive Wiper – used to wipe hard drives to ensure no contamination of information
- Laptop – used at the premises to provide a known process base for imaging and analysis
- Media (CD-ROMs, Diskettes, DVDs, hard drives, USB drives, etc.) – used to store relevant digital information or to leave copies of digital information at the premises
- Network Equipment (cables, card, hub) - used to image hard drives or to communicate between laptops while at the premises
- Network Storage – used in the office to store the digital information to be analysed or shared
- PC (Personal Computer) Cards – used to connect different devices to a laptop
- Server – used in the agency office to store electronic evidence and facilitate the sharing of digital information among officers
- Tool kit (screwdrivers, pliers, etc.) – used to open computers / laptops at the company
- Hardware Write Blockers – used to ensure that digital information is not changed during the review and acquiring process

7.2 Specific computer forensic areas

Most agencies use either dedicated rooms or computer forensic laboratories for processing and analysing digital evidence. These labs are separated from the agency's computer network system (stand alone) and are only used for Forensic IT tasks. Some agencies have developed small internal networks with workstations or, in the analyzing phase, with access possibilities from normal workstations.

7.3 Practices and Procedures

Transparency of computer forensic practices and procedures will assist in ensuring that their use in an investigation can withstand challenge. Most agencies have indicated that they have developed or will develop internal policies and procedures with regard to the collection and analysis of digital evidence.

The following are practices and procedures referred to by agencies in their responses. It is by no means what all authorities do or should do. It should not be considered as a list of best practices. The purpose of the following is to provide an overview of the range of basic practices and procedures followed by agencies.

7.3.1 General

Practices and procedures should comply with overarching established forensic principles. These include ensuring:

- Lawful collection of information (legality principle);
- All involved officers know the procedures;
- Proper storage of information (security and integrity principle);
- Chain of custody (authenticity principle);
- Reproducible results using up-to-date forensic software;
- Validation of the integrity of the data;

- Auditing functions of forensic software are used to produce reports;
- Logs of every action are maintained;
- Use, if applicable, of recommendations from international bodies (such as the Scientific Working Group on Digital Evidence or the International Organization on Computer Evidence);
- Procedures are adapted to the specific case, if possible and applicable;
- Coordination of external computer forensic experts by the authority's own forensic specialists; and
- Quality by reviewing standard operating procedures.

7.3.2 Preparation

7.3.2.1 Searches, Raids and Inspections

Some agencies need a search warrant or court order, which is described in section 4, Legal Authority.

Almost all agencies reported doing physical preparation for a search, raid or inspection. This also includes preparation by intelligence and briefing.

Pre-search, raid or inspection intelligence:

Based on the answers the following actions regarding pre-search are mentioned:

- Seek all available information about the companies' computer systems and infrastructure.
- Seek all available information about the companies' case-related employees.
- Seek all available information about the companies' IT staff.
- Seek all available information related to the location of the server.
- Seek available information about companies' used cloud computing including web-based email and offsite data storage.
- Provide officers with technical information related to the collection of digital evidence.
- Use anonymous web access for internet inquiries to company information. This will not leave traces that can warn the suspected companies.

Physical preparation:

Based on the answers the following actions regarding physical preparation are mentioned:

- Ensure that all media to be used are forensically wiped clean and formatted.
- Ensure that all software to be used is updated.
- Ensure that all hardware to be used is validated and functioning properly.
- Make use of "fly-away kits" (boxes with all needed equipment), to be prepared for digital searches, raids or inspections anytime. These should include hardware, software, forms and written procedures.

Search, raid or inspection briefing:

Based on the answers the following actions regarding briefing are mentioned:

- Provide information to search teams about (new) technologies and devices to store digital evidence that may be found at a search, raid or inspection premises. (iPods, memory cards, WiFi hard discs and other wireless devices, smartphones, USB devices, etc.)
- Provide advice to the search teams as to the correct handling of electronic media and digital evidence located at the search site.

- Discuss with the lead officer the search strategy to be used.
- Provide the team with a contact person (be it the team leader or some other person) who can assist with questions, which may arise during the search with regard to the digital evidence.
- Specify the digital information to be collected including keywords for search.
- Specify the names of persons who are targets including key email accounts.
- Have computer forensic specialists targeting computer systems.

7.3.2.2 Compelled Discovery

Some agencies reported having done the following in preparation for gathering digital information by way of compelled discovery:

- Use the subpoena or document request to define certain terms (e.g. broadly defining the term "document") and set out instructions on how electronic data should be preserved and the digital format in which the data should be produced.
- Give detailed instructions on what steps a company must take to preserve potentially responsive digital evidence.
- Give instructions on how companies must produce digital evidence in a digital format.

7.3.3 Chain of evidence / authenticity

> **It is good practice to document every step taken in the digital evidence gathering process.**

The chain of evidence relates to how the digital information is gathered, processed and analysed. In most jurisdictions it is necessary to have a valid record of the authenticity of the digital evidence, or proof that the digital evidence is unequivocally identical to the acquired digital information, in order for the digital evidence to be legally admissible. The following are examples of methods used by some, but not all, agencies to ensure and demonstrate the authenticity of the digital evidence:

- Preserve digital information as originally acquired;
- Verification by hash values of all digital information;
- Use write blockers when making copies or images;
- Logging of all actions must be part of the documentation;
- Use CD-ROMs with serial number;
- Describe possession of data, equipment, data carriers etc.;
- Make forensically sound bitstream copies;
- Use dedicated forms for documentation; and
- Have written statements of the company to declare the seized digital information is in its original state.

7.3.4 Chain of custody

Chain of custody is the record of the custodial history of the evidence. In most jurisdictions having a valid record of the chain of custody, or describing who has had physical possession, and why and where they had physical possession, is required for legal admissibility of the evidence in court. The following are examples of methods used by some, but not all, agencies to ensure that there is a valid chain of custody of the digital evidence:

- Keep a documented record of the receipt, possession and use of digital information, in some cases this may be countersigned by both the party and the agency;
- Logging of all actions must be part of the documentation, which can be used in any statement or affidavit;
- Make photographs and film recordings of the premises and the handling of equipment on the premises;
- Seal media to be taken from the premises and document this;
- Document opening of seals, if any, for processing in house;
- Record the location of PCs, media etc., to be seized;
- Identify users of hardware, software and media. No doubt should remain;
- Use dedicated forms for documentation; and
- Label all handled materials.

7.3.5 Gathering

It is good practice to establish control of the company's digital information in order to prevent destruction of digital information and evidence.

It is good practice to seek the company's systems administrator's cooperation as the administrator is generally an important person with regard to digital evidence gathering.

It is good practice to solicit information about the computer systems, devices, access codes and practices and procedures for backups, destruction and retention of digital information.

Some agencies must return non-relevant materials to the company while other agencies must delete non-relevant digital information.

The following practices or procedures generally apply to searches, raids or inspections, but may also apply to compelled discovery in certain circumstances.

Although there seems to be a great deal of common practice (and common sense), agencies responded very differently on this item from general good practices through to descriptions of local policies.

- Be prepared for unforeseen situations.
- Inspections, raids and searches should not be carried out without the presence of representatives of the company being inspected, raided or searched.
- Command and control of search, raid or inspection site established by team leader.
- Supervise the local system administrator during the entire process.
- Have prepared a policy about bringing down servers or not.
- Do not switch on hardware that is switched off.
- Describe the location of all machines and data carriers.
- Describe the characteristics of all machines and data carriers. Register BIOS settings (time) of machines.
- Look for documentation, including operating instructions, manuals and service records of systems and software, on the premises.
- Find and gain cooperation of the system administrator, or other custodian of information with regard to programs, systems, data or storage devices who can provide the person(s) authorized to execute the warrant with passwords, log-on codes, encryption keys or other security devices relating thereto.
- Use antistatic bags for transporting data carriers, media and parts.
- Preserve a full copy of the collected material for the company.
- Look for the presence of “wipe software”. This may also be part of the analysis of the digital evidence.
- Look for backup media, such as tapes.
- Check databases and information systems: specifications, data model and ask for ad hoc queries.
- Look for fax software and servers.

Some agencies perform live forensics during on-the-spot investigations. One agency stated that this has the advantage of less processing and analysing at the agency’s office. However, another agency remarked that live forensics may be very time consuming and that in some circumstances an extended search may be unreasonable from a legal perspective. Furthermore the results of paper search will not be available at that stage, limiting the effectiveness of any keyword search.

Further problems were identified with regard to collecting data from different data carriers or data carriers of third parties (e.g. Internet service providers). In some jurisdictions such third parties can be requested to provide the relevant information, whereas in other jurisdictions the rules do not differ substantially from the rules that concern collecting data from the inspected company itself. In the latter case the authorities may require a new search warrant (this may also be due to the fact that this kind of data may not be physically stored at the company inspected). With regard to the collection process as such many authorities reported that the process of collecting, i.e., the copying of data, does not differ from collecting data from the parties inspected.

7.3.6 Preservation of Digital Evidence

Most of the agencies take some measures to prevent deletion of digital evidence. However, even if some of the data was deleted, agencies may have the possibility to retrieve this information with forensic software.

7.3.6.1 Searches, Raids and Inspections

The following measures are taken by agencies to prevent deletion of digital information during a search, raid or inspection:

- A number of agencies reported that when entering the premises, personal computers, data carriers and other relevant electronic equipment and network cables are unplugged. Most agencies do not shut down entire servers. However, personal computers are typically turned off with a hard shut down to avoid deletion of temporary internet files.
- One agency reported that "upon entry to the premises, establishing control is one of the first priorities. In the context of digital evidence, controlling the premises may require that computer users be moved away from keyboards of computers identified as key search priorities and that portable data carriers covered by the search warrant be collected and held under the control of an officer until such time as they have been examined. The search team leader will request the company official to direct company staff not to impede the inquiry by deleting, destroying or removing any records (including digital records) from the premises covered by the warrant during the course of the search. The Act requires the company official to allow the officer searching at the premises to use or "cause to be used" any computer system at the premises."
- One agency explained that different methods are used to prevent deletion. These means are decided on-the-spot depending on the investigation context. Mailboxes may be locked at the server level, equipment (PC, laptop, floppies, CD-ROMs) may be locked in a secure and sealed place until examination or server backup media may be seized during the investigation.
- Some agencies reported the possibility to seal premises and information storage media during the inspection.

7.3.6.2 Compelled Discovery

One agency reported that digital information must be produced in "read-only" digital format so there is no chance that it might be inadvertently changed or deleted by the agencies or investigative staff. Finally, staff make copies of the electronic media (e.g., CD-ROMs) containing the digital evidence as soon as it has been received by the agency. The "original" copy of the media is then secured with other important documents and will not be examined or reviewed for evidence; thereafter, staff handle only the "working copies" of the media (i.e., a duplicate CD-ROM).

7.3.7 Obstruction

It is good practice to have digital evidence gathering practices and procedures that inhibit and help prevent destruction of digital evidence and obstruction.

Several agencies provided information on mechanisms that are in place to guard against obstruction of the search, raid or inspection:

- One agency reported that during the execution of the search warrant, the team leader will advise the company official of the obstruction provision under the Act, namely, that a person who impedes an inquiry or who contravenes a search warrant by refusing to provide access to the premises and the computer systems covered under the search warrant is guilty of the offence of obstruction.
- One agency gave a detailed account of the mechanisms implemented to safeguard the digital evidence. These mechanisms include *inter alia* ensuring that no unauthorised person has access to any electronic devices at the search scene; unplugging the network cables from the computers; taking care to ensure that storage devices are protected from static electricity and magnetic fields; and packing all digital evidence in antistatic packing and in a manner that will prevent it from being bent, scratched, or other-wise deformed.
- One agency reported that it explains the purpose of the investigation and the agency's powers to the most senior person on site, and obtains verbal assurances that nothing will be deleted or destroyed. Furthermore, members of the investigating team are stationed near to key workers' desks to ensure they do not amend or destroy evidence.

Other methods mentioned include the following:

- Isolate people and equipment in a search, raid or inspection to prevent obstruction and destruction of digital information and evidence; and
- Lock mailboxes at server level.

A number of agencies reported that the destruction of digital evidence constitutes an offence that can lead to criminal and/ or administrative sanctions. This fact is conveyed to the company's employees, e.g. one agency reported that the highest ranking member of the staff of the company (normally the CEO) is told that the deletion of any material is strictly prohibited.

7.3.8 Processing

It is good practice to work on duplicates and not on the originally-acquired digital information for ensuring the chain of custody / evidence.

It is good practice to keep data and forensic images until the case is closed, all defendants are successfully prosecuted or all appeals are exhausted.

Processing may include extracting of forensic images, e-mails, zip files, etc., filtering of “known files” or other non-relevant recognised files, decryption, indexing, etc. In general, images of data carriers (made at the premises during a search, raid or inspection) need processing afterwards. In general, copies of individual files and folders, like in compelled discovery, need less processing. Processing of data means to make available and/or visible the collected digital information for investigating purposes.

Most authorities make duplicates of the originally acquired digital information before processing to avoid changing the hash values and thus breaking the chain of evidence.

The following are some other processes that were mentioned:

- Search for deleted files, partitions, file systems, e-mails etc. This may also be part of the investigation process together with reconstitution of deleted files;
- Make sure officers have read-only access for review of digital information;
- Use decryption software if applicable; and
- Ask inspected companies for passwords/ encryption keys if applicable; otherwise use of cracking techniques for passwords.

All agencies generate reports or log descriptions during the processing about actions or steps taken. Some agencies use internal standards for reporting. At the agencies where they use outsourcing in the processing the service providers must maintain a log of their actions which then is used in the preparation of any statement or affidavit.

7.3.9 Analysing

The most used method for analysis is still keyword searching to find relevant documents. With the constant change of technology this may however change.

Keyword search:

- Use pre-determined search queries (keywords, file attributes).
- Use information from informants and witnesses and from interviews on the premises during the search, raid or inspection to formulate key words.
- Use information from analysis of the paper documents collected during the search, raid or inspection.

The following are other analytical options mentioned:

- Review all digital information.
- View the print spoolers.
- Test file signatures, looking for bad files signatures.
- Search for encrypted information. Use decryption tools for encrypted information, if necessary.
- Review registry files, cache files, internet history file and favourites.
- Investigate traces of web chats, webmail, etc.
- Investigate file and folder structure with visual inspection.
- Compare hash values to confirm if there are multiple copies of the same documents.
- Looking for connecting documents.
- Using search strings, code words.
- Use of intelligence software to provide link analysis.

Forensic specialists report to officers about the relevant digital evidence, including whether there are gaps in information, such as none or extremely few e-mails during a certain period or from a certain employee. A cleanly installed hard disk should also be noted. This may also be part of the gathering process.

Most agencies generate reports or logs about all steps during their analyzing work including the list of keywords and its results and the methods of the search used. These reports are extremely important for the chain of evidence. Some agencies use internal standards for reporting. At the end of the analyzing phase some agencies compile a final investigative report about the search results and put the selected documents and evidence in the case file.

7.3.10 Storing information after case closure

After case closure it is of vital interest to the subjects of the investigation what happens to the digital information gathered during searches and raids. One agency reported that the forensic image had been destroyed after the search but before the case closure, which made it impossible to refute some of the companies' challenges in court.

Some agencies must return all digital information to the company after case closure while others are required to delete the digital information. This depends on whether the material is an original or a copy. Some agencies are required to store the information gathered or a copy thereof either permanently or temporary. Sometimes only hard copies are kept whereas in other cases the data is filed.

Some agencies keep the "original" images to the end of the legal proceedings. Therefore the non-relevant documents are deleted from the working copy when the investigation phase is finished. They remain at the agency on the original images, however access to them is strictly limited.

8 LEGAL ISSUES CONCERNING DIGITAL EVIDENCE GATHERING

8.1 General

It is good practice to be cautious in drafting the scope and wording of terms in search warrants or record production orders.

It is good practice to keep in mind the principle of integrity and authenticity of digital evidence during the entire proceedings.

Legal issues mainly concern the authority of the agency to retrieve digital information from the company. This is of course an issue strongly related to the powers of the agencies laid down in their national law. Therefore this section cannot and will not go into detail on the different national regimes and powers, but will look into the more general approaches relating to the legal issues as came forward from the answers to the questionnaire. These issues relate to the way the powers for digital evidence gathering are set out in national legislation, the handling of legally privileged and private digital information and the power to get physical access to digital information stored outside business premises or even outside the jurisdiction of agencies. In some cases agencies may have written guidelines how to deal with these issues.

It is a general legal issue at all agencies concerned with digital evidence gathering and processing to keep in mind the principle of the integrity and the authenticity of the digital evidence during the entire proceeding.

With digital information getting more and more importance and attention, a number of court cases were reported. Agencies reported cases dealing with a wide range of issues and differences due to specifics of the jurisdictions. These issues range from the question of copying large quantities of electronically stored data in general to specific questions on the scope of the Legal Professional Privilege. One agency reported a judgement that only data that can be linked to the suspected infringement may be copied and further explored. The company must be able to claim and verify the separation of relevant and non relevant data. The coming years will be marked by important decisions in different jurisdictions, which will help to define the scope and the competences of the national authorities in the different jurisdictions.

8.2 Power for digital evidence gathering

Of the responding agencies, 92 % stated that their national law gave them the power to perform digital evidence gathering, either by way of searches, raids or inspection or by way of compelled discovery. In almost all jurisdictions this power is interpreted from an already existing power to compel or seize documents relevant to an ongoing investigation.

As technical developments are rapid, the fact that almost all jurisdictions derive their power from an interpretation of already existing powers seems a good practice. To lay down special powers for digital evidence gathering in national law today may run the risk that tomorrow's technical development(s) will restrict them in their possibilities.

It seems that because the authority to gather digital evidence is based on an interpretation of already existing powers, a parallel is sought with the traditional gathering of hard copy documents. For now, this may be a well-functioning approach. However in the future this could lead to a restriction of the possibilities digital evidence gathering can provide as new approaches not purely related to documents may emerge.

One agency with a specific provision assumes that they can evolve with technology. Furthermore, recent developments have shown that having a specific legal provision has not led any agency to report negative experiences. It will remain to be seen how this develops further.

8.3 Handling of legally privileged and private digital information

It is good practice to have a systematic approach for the review, selection and handling of privileged and private and potentially privileged and private digital information.

In many jurisdictions, correspondence between the company and a lawyer is protected by legal privilege. Furthermore many agencies are not entitled by law to seize or copy private documents, such as private correspondence, photographs etc. These documents (legally privileged and private) are generally not to be seized or copied or compelled by agencies. In the case of hard copy documents there exist well known ways to ensure that these documents are not seized or copied by the agency. By looking at the header of the document and/or the rough content, an officer can generally determine whether a document is legally privileged or private.

In the case of digital evidence gathering during searches, raids or inspections, the content of the documents cannot always be studied or looked into at the business premises. The data carrier on which the digital information is stored will often be copied and further examined at the office of the agency. The handling of privileged and private digital information will therefore sometimes differ from the handling of hard copy documents.

In addition, the scope of legal privilege differs between jurisdictions. Most agencies recognise documents as legally privileged when they concern correspondence between a lawyer and his client. One agency only recognises documents as legally privileged when they concern correspondence between a lawyer and a client that is in the possession of the lawyer or correspondence between a lawyer and a client that concerns the defence of the client (thus after the start of proceedings).

The following describes the way privileged and private documents are generally handled by agencies in the context of digital evidence gathering. This description focuses on digital evidence gathering during searches, raids or inspections. In the case of digital evidence gathering by compelled discovery, problems with privileged or private digital information are rarely encountered.

Most jurisdictions are not allowed to seize or copy legally privileged or private documents. These agencies first try to extract the legally privileged or private documents from the data carrier and then make a copy of the data carrier. For instance, if digital evidence gathering copies are made at the premises of smaller stand alone digital carriers (floppy discs, USB devices, etc.), an official of the company may point out which documents on this device are likely to be legally privileged or private. The agency will judge the validity of the claim in a *prima* facie assessment and, if approved, these documents can be removed from the device to be copied. In case of disagreement, a formal protest can be made or the company can go to court to fight the judgement of the agency.

If digital evidence gathering images are made from data carriers, it is not possible to remove documents that are legally privileged or private. The reason for that is the nature of an image: an exact bit-by-bit copy of an entire data carrier. In the case of copies of larger digital devices, it may be impossible to remove all privileged or private digital information at the premises of the company. This may restrict some agencies in their ability to copy bigger digital devices.

In some cases the amount of content on the copy generally is too big to review at the premises of the company and analysis is carried out at the agency's office. Otherwise the stay on the site would be prolonged and may be unnecessarily disruptive for the business of the inspected company. The analysis is done in various ways. At some agencies, before looking at the content of the documents - as in the case of an image - a company and its lawyer will be invited to the agency's office to come forward with the names of the documents containing legally privileged or private digital information. These documents will then be selected and an assessment will be made as to whether the documents are legally privileged or private. This assessment may be conducted by one of the officers on the case or by someone who is not involved in the investigation. Documents that are legally privileged or private are destroyed or returned to the company. The remaining digital information on the copy will be analysed and studied by the agency. In case of disagreement, a formal protest can be made or the company can go to court to fight the judgement of the agency.

Some jurisdictions have a special provision in their law to deal with claims of legal privilege. In these jurisdictions the records on which the company claims legal privilege, may be copied to separate media and sealed pending an agreement being reached about the claim between the Counsel of the company and the agencies. Sometimes an independent third party or even the court will decide about the claim. Such an independent third party may consist of personnel from another location of the agency or other agents not working on the case.

8.4 Physical access to digital information

As digital information can be easily transmitted from and stored in places different from those physically inspected, one of the legal issues is whether agencies have access to and can copy digital information stored on a server outside the business premises.

Three different situations can be distinguished:

- a situation in which the server (digital information storage) is not located at the (specific) premises of the company inspected, but at another premises of the company;
- a situation in which the server (digital information storage) is not located at the premises of the company inspected but at the premises of another company contracted for this storage (third party); and
- a situation in which the server (digital information storage) is located outside of the territory of the agency.

There are two general approaches:

Some agencies look at the fact whether the company searched, raided or inspected has access, uses and controls the information stored at the other business premises of the company. If the company has access, uses and controls the digital information, the digital information is regarded as being at the searched, raided or inspected premises and access is permitted and copying done. The location where the digital information is stored is no issue. This approach can be called “the Access approach”.

Other agencies will purely look at the location where the digital information is stored. If this location differs from the one described in their legal order (court order, administrative decision, etc.) they must get a new legal order to obtain access and be permitted to copy the digital information. Therefore some agencies describe the premises to be inspected in such a way that it covers as many premises of the company involved as possible within its jurisdiction. This approach can be called “the Location approach”.

In this chapter the consequences of the two approaches are given for both situations.

8.4.1 Digital information stored outside the companies inspected premises

In some cases inspectors will find that the digital information is stored outside the inspected premises of the company. Agencies answers on how to deal with these situations differ, according to where exactly the information is stored.

8.4.1.1 Another premises of the same company

In the Access approach the agency will have access to digital information stored at other premises of the same company if the searched, raided or inspected company has access, uses and controls the information at the other premises.

In the Location approach the agency will need a new legal order to get access to the information. Describing the premises to be inspected in such a way that the description covers as many premises of the company involved as possible avoids the necessity to obtain a new legal order in the course of the investigation.

8.4.1.2 Premises of another company

In the Access approach, if the company inspected has access to, uses and controls the digital information, the digital information is considered to be accessible at the searched, raided or inspected premises and access is allowed.

In the Location approach the agency will need a new legal order to get access to the digital information, as the original legal order covered a different location. A broad description of the premises of the company involved will not overcome the barrier for access as the location of the digital information concerns another company (third party).

8.4.1.3 Digital information stored outside the territory

If the agency follows the Access approach, when the company searched, raided or inspected has access to, uses and controls the digital information, the agency has, through the searched, raided or inspected premises, access to the digital information in the other territory.

Agencies that follow the Location approach will not be allowed to access the information stored outside the territory. In these cases the agencies use the possibility of mutual legal assistance treaties or agreements to gather the digital evidence.

8.5 Using digital evidence in court

Agencies may introduce the digital information gathered in different ways during the course of the investigation and at trial. Most agencies have not encountered significant legal problems in using the evidence gathered in court. However not all agencies have used the digital information gathered in court proceedings.

9 ADVANTAGES AND FUTURE CHALLENGES

Most agencies indicated that digital evidence gathering was advantageous for getting access to significant information. A number of agencies mentioned that digital evidence gathering allowed access to large volumes of data, which in itself may prove to be an advantage as well as a disadvantage.

Some examples of advantages:

- One agency reported that the main advantage is that information about the firm's competitive strategy and communication between the competitors are usually found on digital media.
- One agency reported that the main advantage with making forensic images is the possibility to restore erased data. This enables the authority to collect evidence of an infringement even if the dawn raid was expected and the company has been 'cleaning up'.
- One agency reported as an advantage that extra-time and resources were granted by post-inspection analysis.

Some agencies advised that digital evidence gathering contains challenges as the agencies have to keep up with the companies' rapid advance in technology. Furthermore one agency warned that keyword searches can be thwarted through the use of code words or intentional misspellings. Finally, some agencies mention the lack of sufficient resources – be it IT staff, hardware and software and training – as a challenge to be overcome in the future.

APPENDIX 1 GOOD PRACTICES RELATING TO DIGITAL EVIDENCE GATHERING[4]

The following list reflects key practices common to many of the competition agencies responding to the SG 2 questionnaire that formed the basis for this Chapter. This list is meant to provide a concise summary of common practices in the conduct of the digital evidence gathering. The list does not purport to present all possible practices, nor does it necessarily recommend these practices over others. Practices will depend on the peculiarities of each jurisdiction's cartel regime and the particular circumstances.

RESOURCES FOR DIGITAL EVIDENCE GATHERING

It is good practice:

- to have a dedicated internal organisation or staff capacity to undertake digital evidence gathering.
- for officers and forensic specialists to work closely during all stages in the gathering of digital evidence.
- to give special training to the agency's staff who collect digital evidence.
- to describe the scope and nature of cooperation with other public agencies in a protocol.

THE ELEMENTS OF DIGITAL EVIDENCE GATHERING

It is good practice:

- to use tools that are thoroughly tested and generally accepted in computer forensics.
- to document every step taken in the digital evidence gathering process.
- to establish control of the company's digital information in order to prevent destruction of digital information and evidence.
- to seek the company's systems administrator's cooperation as the administrator is generally an important person with regard to digital evidence gathering.
- to solicit information about the computer systems, devices, access codes and practices and procedures for backups, destruction and retention of digital information.
- to have digital evidence gathering practices and procedures that inhibit and help enforce against destruction of digital evidence and obstruction.
- to work on duplicates and not on the originally-acquired digital information for ensuring the chain of custody/ evidence.
- to keep data and forensic images until the case is closed, all defendants are successfully prosecuted or all appeals are exhausted.

[4] Please note that good practices set out in other Chapters of the Anti-Cartel Enforcement Manual may also apply to digital evidence gathering.

LEGAL ISSUES CONCERNING DIGITAL EVIDENCE GATHERING

It is good practice:

- to be cautious in drafting the scope and wording of terms in search warrants or record production orders.
- to keep in mind the principle of integrity and authenticity of digital evidence during the entire proceedings.
- to have a systematic approach for the review, selection and handling of privileged and private and potentially privileged and private digital information.

APPENDIX 2 RESPONDING AGENCIES

Competition agencies from the following jurisdictions responded to the questionnaire (see Annex 3) which served as a primary source of information for this Chapter:

1. Australia
2. Brazil
3. Canada
4. Cyprus
5. Finland
6. Germany
7. Hungary
8. Ireland
9. Italy
10. Japan
11. Mexico
12. Netherlands
13. New Zealand
14. Norway
15. Pakistan
16. Peru
17. Poland
18. Romania
19. Russia
20. Spain
21. Sweden
22. Switzerland
23. United Kingdom
24. United States

APPENDIX 3 QUESTIONNAIRE

INTERNATIONAL COMPETITION NETWORK

CARTEL WORKING GROUP

DIGITAL EVIDENCE GATHERING: UPDATED QUESTIONNAIRE

Agency Name:	
Contact details (contact person, e-mail address):	
Date:	

NOTE: Please be advised that (i) the following is an updated version of the original survey done in 2005 and (ii) Agencies who have responded earlier are free to refer to their former response by attaching it and to update their response to the questions in BOLD. Of course, Agencies who are new respondents will wish to respond to the entire survey.

- Confidentiality: In determining the level of detail to provide in your responses, please keep in mind that the information you provide will be used for the purposes of drafting the Anti-Cartel Enforcement Manual's chapter on digital evidence gathering and for discussion at the Cartels Workshop. As a result, the confidentiality of the information cannot be guaranteed. Note that therefore no confidential information should be given in the answers.
- Repeated information: If you have already provided similar information elsewhere, please simply indicate this under the relevant question(s) on the questionnaire and attach this information to your submission.

DEFINITIONS

- **Computer Forensics** is the use of specialized techniques for the preservation, identification, extraction, authentication, examination, analysis, interpretation and documentation of digital information. Computer forensics comes into play when a case involves issues relating to the reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer Forensics requires specialized expertise that generally goes beyond normal data collection and preservation techniques available to end-users or system support personnel.
- **Digital information** is all information in digital form and can be divided into the content itself (of a text document, a drawing or photo, a database, etc.), and the information about this content, the so called metadata (filenames, pathnames, the date and time that a document has been created or edited or an e-mail has been sent, received or opened, the creator/ sender of a document or e-mail, etc.). It is often not possible to handle digital information without acquiring knowledge of at least some of this metadata.

- **Digital evidence** is all digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the storage media (data carrier), the tapping or monitoring of network traffic, or the making of digital copies (forensic images, file copies, etc.), of the data held. Although hard copy print outs of digital information are not digital evidence in the strict sense of this definition, it is considered a starting point for applying digital evidence gathering in the future.
- **Forensics** is the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for a court of law or other legal context.
- **Chain of custody** is the record of the custodial history of the evidence.
- **Chain of evidence** or authentication is the record of the collection, processing and analysis of the digital evidence. It proves that the presented evidence is unequivocally derived from the acquired digital information.
- A **data carrier** is any device that contains or transports digital information and includes a physical hard drive, a floppy disk, Personal Digital Assistants (PDAs), Universal Serial Bus devices (USB's), a sim-card from a cell phone, a flash memory stick/card, a network and a server, etc. This list is non-exhaustive.
- A **hash value** is a mathematical algorithm produced against digital information (a file, a physical disk, a logical disk) thereby creating a digital fingerprint for that information. It is by purpose a one-way algorithm and thus it is not possible to change digital evidence, without changing the corresponding hash values. In other words, if the hash value of a file has (not) changed, the file itself has (not) changed.
- A **forensic image** (sometimes called a forensic copy) is an exact bit-by-bit copy of a data carrier including slack, unallocated space and unused space. There are forensic tools available for making these images. Most tools produce information, like a hash value, to ensure the integrity of the image.
- **Live forensics** is a technique that consists of performing analysis on live systems (running) to extract information from live memory (information which is lost when the computer is powered down)

GENERAL QUESTIONS

1) Please describe the possibilities available to the competition authority for collecting digital evidence (e.g. during dawn raids, compelled discovery, etc.).

2) Is there an explicit legal basis for collecting digital evidence or is it a question of interpreting of existing powers of investigation? Does this legal basis apply to the collection of all forms of digital evidence? If there is a legal basis when did this enter into force?

3) Has the competition authority already used its powers to collect digital evidence?

If the national authority is authorized to collect digital evidence and has experience in this area, please answer the following questions.

QUESTIONS REGARDING THE COLLECTION OF DIGITAL EVIDENCE

4) Does the competition authority have a dedicated computer forensics laboratory? If so, are there any accreditation processes your agency has complied with in setting up such a facility? If not, please explain what your organisation uses instead to analyze digital evidence, and whether there are reasons that the competition authority does not have a dedicated computer forensics laboratory.

5) With regard to the staff within your organisation dealing with the collection of digital evidence: Please describe a.) their functions and qualifications/expertise (e.g. IT-- specialists, officers), b.)

the training they receive (internally or commercially sourced) and c.) their placement within the organisation (e.g. separate unit).

6) Would you or do you contract out or assign any part of the collection or analysis of digital evidence to third party private companies or to other public agencies? If so, to what types of companies or agencies, at what stage of the investigation process and under what circumstances? Are there any special requirements for dealing with confidentiality and security issues?

The digital evidence collection process can be divided into several phases. In this questionnaire the following five phases are identified: preparation, collection, processing, investigation and closure. If applicable, please answer the following questions. If you identify different phases, please describe those phases and (try to) answer the following questions:

PREPARATION

7) What is the necessary legal basis for collecting digital evidence (e.g. court order, decision made within the competition authority)?

8) What preparations are made specifically for collecting digital evidence (e.g. inspection briefing, physical preparation, consulting with forensic experts)?

9) Are there any overarching binding or advisory standards or laws that must be considered when either collecting or analysing digital evidence in your jurisdiction?

10) Does the competition authority have its own internal policies and procedures for the collection and analysis of digital evidence?

COLLECTING DIGITAL INFORMATION

11) Which member(s) of staff is eligible to conduct the on-the-spot investigation and collection of digital information?

12) What kind of tools do you use for collecting digital evidence (software and hardware)?

13) Please describe, if applicable, the level of cooperation required of the company involved (e.g. support of company administrator) and how this cooperation is ensured.

14) Is the competition authority authorized to collect digital evidence from an external server that is a.) physically located outside the company inspected, b.) outside your country or c.) stored at another company (e.g. service provider)? If so, please describe the legal basis and, if applicable, any special requirements that have to be met.

15) What are the procedures for collecting data from different data carriers or data carriers of third parties, such as internet service providers? To the extent that the procedures may differ depending on the nature of the third party or the type of data collected, please respond separately as to each.

16) Do you examine other types of digital devices for possible evidence (e.g. Smartphones, Cell Phones, PDAs, USB devices etc.)? Please explain.

17) Do the competition authority's procedures for collecting and preserving digital evidence from third parties differ from the procedures used to collect and preserve digital evidence from the subjects of the investigation? If so, please explain.

18) Please describe, if any, the procedure to be followed at on-the-spot investigations for preventing the deletion and/or destruction of digital evidence? Should different procedures apply to on-the-spot investigations in your jurisdiction, please explain the general procedure to be followed for preventing the deletion and/or destruction of digital evidence.

19) What is done to ensure (and to be proved at a later date) that the gathered information was at the time an accurate and complete copy of the original (chain of evidence)? Are there written procedures or instructions for this process?

20) How is the possession and handling of digital information (chain of custody) recorded? If any documentation (for internal or external use), e.g. a written report/record, is made of the collection of the digital information, please describe.

21) Do you cooperate with other authorities in collecting and/or analyzing digital evidence (e.g. police)?

22) Do you conduct live forensics at all? How is data handled on site (e.g. Bag and tag operation, image everything, preview and image if necessary, search and seize relevant data only)? Please explain. Note: some options take progressively longer on-site during the collection process, but require less time during the investigation process.

PROCESSING DIGITAL INFORMATION (RESTORE DATA, UNZIPPING, BACK-UP AND FILTERING, INDEXING AND/OR RETRIEVAL OF INFORMATION)

23) What is the background/qualification of the staff processing digital evidence (e.g. IT experts, officers)?

24) Please describe the procedure for processing digital information.

25) What tools do you use for processing digital evidence (software and hardware)?

26) What documentation (for internal or external use), e.g. a written report/record, is created while processing the digital information? Is this based on internal standards or on law?

INVESTIGATION PROCESS

27) What is the background/qualification of the staff investigating and analyzing the digital evidence (e.g. IT experts, officers)?

28) Please describe the procedure (methods) of investigating and analyzing the digital information for evidence. In other words: What steps are taken to find evidence in the digital information?

29) What tools do you use for investigating and analyzing digital evidence (software and hardware)?

30) What documentation (for internal or external use), e.g. a written report, is created while analyzing the digital information?

31) What are the legal aspects to be considered when investigating and analyzing the digital evidence? Note: please specify any legal considerations with regard to the analyzing and the further issues such as chain of evidence etc.

32) What happens to data that is irrelevant for antitrust purposes?

CASE CLOSURE

33) What procedure does the competition authority follow in relation to the collected digital data after closing the investigation (e.g. by statement of objections or because of a successful prosecution or because no competition infringement could be found) or in the case of definitive closure of the file? What does the national law prescribe in this regard? What happens to the digital information collected during the investigation (returned to the companies involved, destroyed, filed, etc.)?

MISCELLANEOUS

34) Has the competition authority encountered any specific legal problems or issues in the course of collecting digital evidence? If possible, provide a short description of these legal problems or issues, including a summary of national judgments or court decisions if applicable.

35) How does the competition authority deal with legally privileged or otherwise legally protected documents when collecting and/or processing digital evidence?

36) Has digital evidence been used as key evidence in any recent cases in your jurisdiction? Has the competition authority experienced any problems with introducing digital evidence in administrative or judicial proceedings? If so, please provide details.

37) Where do you see the main advantages or disadvantages of your digital evidence collection process? How could things be improved?

ADDITIONAL COMMENTS:

38) Please feel free to elaborate upon or provide additional observations, comments or information.