Cartel Enforcement Subgroup 2- ICN Cartels Working Group
Anti-Cartel Enforcement Manual

Chapter on Digital Evidence Gathering

Table of 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 competition agencies to increase the use of digital evidence gathering as a frequent or standard tool in their fight against cartels.

This version of the Chapter represents a second revision. The previous version of the Chapter was released in March 2010, and was based on information collected from ICN members in November 2009 by means of a questionnaire to which 24 member agencies participated. The March 2010 version of the Chapter was an update to the original version, which was published in 2004. This version of the Chapter is streamlined from the two previous versions, and was updated after receiving input from a number of competition agencies and non-government advisors.

The goal of this Chapter is to help readers 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.

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 as well.

This Chapter is intended to be a reference for competition agencies that are undertaking digital evidence gathering in the course of anti-cartel investigations, and is not intended to be a comprehensive guide. The ICN *Anti-Cartel Enforcement Manual* is a work in progress and all Chapters may be updated or revised in the future. This Chapter reflects the current status of digital evidence gathering. As technology, software and hardware change continuously, the definitions used and the methods for collecting, analysing and ensuring the admissibility of digital evidence will also be subject to change.

This Chapter and the others that form the *Anti-Cartel Enforcement Manual* must be read in the context of current enforcement laws, policies and practices of each jurisdiction. Practices which work well in the jurisdiction(s) where they are applied may or may not work well in the legal context of another jurisdiction and, therefore, cannot necessarily be recommended for adoption by other ICN members. This compilation does not purport to present all of the possible practices, nor does it necessarily recommend these practices over others, as the appropriate choice of approach will depend on the circumstances of each particular situation. The relevance and therefore likely adoption by jurisdictions of particular practices outlined in this Chapter will be influenced by their competition policy and law environment. In some cases, certain practices will not be available due to legal, legislative or political regimes in which those competition agencies operate.

2 DEFINITIONS AND QUALIFICATIONS

The definitions mentioned below are meant as points of reference in order to have a common understanding of digital evidence gathering among competition agencies for the purposes of this Chapter.

2.1 Defined Terms

- **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.

- **Chain of custody** is the record of the custodial history of the evidence. It is the process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time the evidence was collected or transferred and the purpose for the transfer.

- **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.

- **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 information technology (IT) system support personnel.

- A **data carrier** is any device that contains or transports digital information and includes physical hard drives, floppy disks, Personal Digital Assistants (PDAs), Universal Serial Bus devices (USBs), SIM-cards from cellular phones, flash memory sticks/cards, networks and servers, etc. This list is non-exhaustive.

- **A deleted file** is a file that has been logically, but not necessarily physically, erased from an operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data. Generally, until data is overwrittten it may be recoverable.

- **Digital evidence** is all information in digital form that may be used as evidence in a case. Digital evidence, such as storage media (data carrier), tapping or monitoring of network traffic, or making digital copies (forensic images, file copies, etc.) may be obtained by searches, raids and inspections, through compelled production or through voluntary production (*see* Sections 5.1-5.3).

- **Digital information** is all information in digital form and can be divided into the content itself (*e.g.* of a text document, a drawing or photo, a database, etc.), and the information about this content, also known as metadata. It is often not possible to handle digital information without acquiring knowledge of at least some of this metadata.

- **Encryption** is the conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

- **Forensics** is the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for legal proceedings (*i.e.* a court of law or other legal context).

- 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 forensic images. Most tools produce information, like a hash value (as described below), to ensure the integrity of the image.

- A **hash value** is a mathematical algorithm produced against digital information (*e.g.* a file, a physical disk, a logical disk) thereby creating a "digital fingerprint" or "digital DNA" 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. Given this role in uniquely identifying digital information, hash values are often used to authenticate computer records introduced in legal proceedings (*i.e.* a court of law or other legal context).

- **Live forensics** consists of seizing or analysing system information, memory contents and/or contents of data carriers from live systems (*i.e.* systems that are on/running). This extracts information from live memory (*i.e.* information which is lost when the computer devices or systems are turned off/powered down).

- **Metadata** is information about a particular data set or digital document, which describes how, when, and by whom the data set or digital document was collected, created, accessed, or modified.

3 THE ADVANTAGES OF DIGITAL EVIDENCE GATHERING

In many jurisdictions, digital evidence has contributed to demonstrating anti-competitive conduct. This evidence can be gathered during searches, raids, or inspections; obtained through compelled production; or acquired through voluntary production, such as the cooperation of a leniency applicant. Digital evidence gathering is a powerful tool for competition agencies in their fight against cartels. It can be used individually or alongside more traditional methods of evidence gathering and should be a standard and regular practice in cartel investigations. Furthermore, digital evidence may help in the course of an investigation to prepare for the next steps in the investigation. While digital evidence in cartel cases can take many forms, some examples have included e-mails confirming coordination by competitors or the recovery of deleted records demonstrating bid rigging.

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

3.1 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 are relying less-and-less on hard-copy documents in favour of storing records digitally. Some hard-copy documents located at a search, raid or inspection site, obtained through compelled production or through voluntary production, such as the cooperation of a leniency applicant, can be a hard-copy print-out of digital information, while other information may never appear in hard-copy format. This information will not be obtained when gathering evidence in more traditional ways.

3.2 Some information in hard-copy was destroyed

Companies under investigation for competition violations may occasionally consider unlawful or inappropriate methods to avoid having agencies uncover evidence that may contribute to demonstrating these infringements. Destroying hard copy documents, while relatively rare, is an easy way of hindering or obstructing an investigation. Although using digital evidence gathering to locate evidence does not prevent the possibility of obstruction of an investigation, it does provide the possibility of recovering deleted or destroyed evidence. In more traditional ways of gathering evidence, this would not be possible. However, it should be noted that it is possible to completely destroy all traces of digital evidence as well.

3.3 Hard-copy information is limited to the content

Hard-copy information can contain important pieces of information or evidence (*e.g.* handwritten notations or fingerprints) that are not available in digital form; however, a hard-copy document is limited to the content of the document. Digital files or programs, on the other hand, contain metadata or data about the digital information, which can give access to a new source of information. Metadata can provide information about the origin, size and format of digital information, including the author of a file and the date when it was created, last altered, accessed or deleted. Metadata may also give detailed information about the revisions of a document. Digital information can also be obtained concerning the exchange of information, the identity of the sender and receiver of the information and what actions individuals have undertaken with this information.

3.4 Hard-copy information may not have all the content

A hard-copy of a document will contain information only in the format that has been selected for printing. A digital copy, on the other hand, may contain additional information such as the calculation formulae used (*e.g.* in a spreadsheet), metadata, comments or visible additions/deletions.

3.5 Better quality input in case management system

Increasingly, competition agencies have been providing their investigation teams with case management software, allowing the team to search the entire case file. A digital document in its native format is likely to provide more comprehensive search results compared to a hard-copy document that has to undergo “optical character recognition” (OCR) for it to become searchable.

4 LEGAL AUTHORITY

The legal basis for digital evidence gathering may be explicitly set forth in the relevant laws or derived from the interpretation of already existing provisions in national laws that permit competition agencies to collect or seize documents.

Competition agencies should carefully check and ensure that they have the authority to request, search or compel business records that are contained on a variety devices (*e.g.* telephones, laptops, tablets and so on) that belong to company employees. It is increasingly the case that companies allow or tolerate a "Bring Your Own Device" policy. These policies are likely to lead to a variety of devices within a company for which even the company's IT system support personnel may provide little or no support, or even have knowledge of their functioning.

Competition agencies should also ensure that they know how to deal with potential objections with respect to access to digital evidence based on privacy and/or telecommunication legislation in their respective jurisdiction.

5 MAIN DISTINCTIONS IN DIGITAL EVIDENCE GATHERING

There are three main practices used by competition agencies to gather digital evidence: searches, raids and inspections, compelled production and voluntary information, which is generally obtained from the cooperation of a leniency applicant.

5.1 Searches, Raids and Inspections

Digital evidence gathering by means of a search, raid or inspection can be carried out in two distinct forms.[1] The first one is by seizure of a data carrier. This data carrier is seized and then fully searched to retrieve digital evidence at the office of the seizing competition agency. Generally speaking, only legal professional privileged information is excluded from the investigation at the office of the competition agency. The exclusion of such privileged information is done by claims of the company or on the initiative of the officials of the competition agency. The handling of legally privileged information is discussed further in Section 8.3.

The other main practice of digital evidence gathering by means of a search, raid or inspection, is by searching the data carrier on site and copying or making forensic images of digital information. The image of digital information can then be examined and analysed off-site at the office of the competition agency.

If the analysis of the collected digital evidence takes place at the premises of the company, the digital information will be searched by means of search strings or other specific intelligence available to the case team of the competition agency and a digital copy of the selected digital information will be reproduced or the selected digital information will be printed. Legally privileged information is directly claimed by the company. This selection of (copied) digital information will then be taken to the competition agency for handling by the case team. The advantage of this method is the availability to the case team of a data set within a relatively short timeframe. The disadvantage is the fact that the case team cannot go back to the copied or imaged information to conduct further searches once more case information has become available. The case team will have to contend with the selection at the premises of the company, even if new intelligence develops during the investigation.

If the analysis of the digital evidence takes place at the office of the competition agency, a selection of the imaged digital information will also be made available through the use of search strings or other specific intelligence available to the case team of the competition agency. Legally privileged information can be claimed by the company over the whole content of the image. The advantage of this method is that the case team can go back to the imaged digital information as new intelligence develops during the investigation. The disadvantage of this method is the fact that, due to the often large amount of data taken from the premises, it may take a relatively long period of time before the case team has access to the selected data set. However, this period can often be utilised by the case team to analyse the hard-copy material seized during the search, raid or inspection and acquire further intelligence that can assist with the analysis of the digital evidence collected.

[1] Although this Chapter primarily focuses on searches, raids or inspections of companies, for purposes of digital evidence gathering, in some jurisdictions such information can also be obtained from an individual and/or his/her premises.

5.2 Compelled Production

Compelled production, whether by subpoena, order for production or request for information, is used to require companies or individuals to produce any requested documents or records – whether hard-copy or digital – that are relevant to an investigation. A competition 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 competition agency that performs a thorough search for all responsive documents and produces them in an acceptable format (which may be dictated by the competition agency, such as native files). During this process, it is important for the competition agency to learn about the computer systems and the efforts made by the company to preserve digital evidence. The search methodology used by the company is also an important factor to be considered.

5.3 Voluntary Production

Competition agencies typically demand complete and continuing cooperation from applicants seeking leniency. Further investigation will be needed to locate all of the cartel participants and assemble the necessary evidence to adjudicate or prosecute, and leniency applicants are particularly well placed to assist in that process. Leniency applicants are often asked to undertake specific tasks, which may include digital evidence gathering, such as forensic imaging of computers of relevant employees.[2]

[2] *See* ICN *Anti-Cartel Enforcement Manual* Chapter on Drafting and Implementing and Effective Leniency Policy (2014) (*forthcoming*).

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 through electronic devices means that staff must be knowledgeable of the latest technological developments and techniques. Therefore, it is important for competition agencies to put effort into training staff. Management must also be supportive of keeping staff informed regarding the latest technological developments and techniques 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 that is capable of undertaking digital evidence gathering.

Some competition 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 may also have a special role in the early examination or analysing phase (*i.e*. indexing or retrieval of digital information).

Other competition agencies have specialists working in their IT department who dedicate part of their time to digital evidence gathering. These IT specialists may also assist case teams during searches, raids or inspections, and the analysis of digital evidence.

As the number of IT specialists within a competition agency can often be insufficient to deal with searches at multiple locations, competition agencies may train some of their case handlers in the basics of digital evidence gathering. These trained case handlers may be used in the collecting phase, and later on, in the processing and investigating phases. During the analysing phase, most competition agencies use case handlers who have received some specialised training, with the support of IT specialists. Digital evidence gathered is thus generally a combined effort of IT specialists and case handlers at different stages of a case.

Outsourcing digital evidence gathering to other public agencies is a practice some competition agencies engage in frequently. This concerns not only the retrieval of digital evidence, but also the analysis of digital evidence. In this phase, however, the outsourced public agency, usually works together with the case team (*see* also Section 6.5).

Outsourcing digital evidence gathering to private companies is a practice used by a minority of competition agencies. Outsourcing such an activity is generally subject to national procurement rules. This practice may entail the retrieval and processing of digital evidence, but hardly ever the analysis of that digital evidence. The companies involved in such work generally must sign either a statement on confidentiality or a confidentiality agreement. In some cases, there are also agreements restricting these companies from working for companies under investigation by the competition agency. It is, however, good practice for those competition agencies that outsource to private companies to maintain a minimum

knowledge within the organisation in order to ensure that the appropriate service is purchased at a reasonable price level.

6.3 Officers and forensic specialists

> It is good practice for the IT staff/forensic specialists to work closely with the case handlers during all stages in the gathering of digital evidence.

When it comes to analysing digital evidence, there should be a close working relationship between the IT-staff/forensic specialists and the case handlers, if the two are separate. This working relationship typically starts at the earliest possible moment in an investigation to ensure that the relevant digital evidence is copied and prepared for analysis in the most effective way. A number of efficiencies may result from early collaboration among the various parties involved. One primary benefit is the early identification and focus on key case issues. Those with law backgrounds bring the perspective and understanding on what is needed for court; forensic specialists are familiar with the tools and data resources that can be used to locate key evidence; and investigators will be aware of key facts in the case. This early teamwork will focus and conserve resources as the case proceeds.

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.

Staff (forensic specialists or officers) practicing digital evidence gathering should receive special training. Forensic specialists are well-trained in using 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 evidence. Most competition 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 forensic specialists in or outside the competition 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 and the International Association for Computer Information Systems provide a venue for the gathering and sharing of information between international forensic specialists and they both provide non-vendor specific training. Several organisations also provide vendor-specific or non-vendor specific certifications.

In order to maintain knowledge on developments, some competition agencies participate in knowledge-oriented networks of national enforcement agencies. For example, European

competition agencies participate in the European Competition Network's Forensic IT Working Group. During these meetings, experiences and best practices are exchanged between the competition agencies' technical and legal experts in computer forensics. Related to this, since 2009, the Italian Competition Authority has promoted a European project of specialized training. Virtually all competition agencies in Europe have participated in one or more of these training projects covering basic and advanced training, exchange programmes and common open-source software development.

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 on digital evidence gathering.

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

Specific points that may be usefully reflected in such a cooperation protocol can be:

- Hours that the other agency will provide and how they will be calculated (overtime on a mission; specific periods and so on); maximum time on mission; training for team
- Material that will be made available: hardware, software, supporting material
- Names and/or qualifications of the staff that will provide the support
- Minimum time period that support staff will be informed before an intervention
- Price of the service/contract
- Duration of contract and review modalities

This protocol should cover the responsibilities and procedures of these agencies during the digital evidence gathering process. Furthermore, they should outline the handling and exchange of retrieved data. An example cooperation protocol can be found in Appendix 2.

6.6 Budget

It is good practice to have a dedicated budget to cover the costs of purchasing and maintaining hardware, software, licensing and forensic tools, as well as staff training.

The set-up, installation and maintenance of digital evidence gathering tools in an appropriate environment, and the continued training of staff, can be costly. Additionally, digital evidence gathering technology is constantly changing and evolving, and these changes may require that a competition agency's tools are updated more frequently. It is therefore advisable, particularly in view of multi-annual planning, to have a dedicated annual budget for digital evidence gathering technology, which includes the purchase and maintenance of hardware, software, licensing and forensic tools, as well as staff training.

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 competition agencies use commercially available computer forensic tools for digital evidence gathering. Some commercial tools may be made available only to "law enforcement agencies". The use of self-developed, open-source software is, in general, limited, although there is a culture of "sharing" amongst the forensic IT experts in the context of their international associations/fora.

Software[3] 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 and duplicators – used to allow the 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 mobile devices;
- 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 competition 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 legal proceedings; and
- Backup Software – used to retrieve or produce a copy of digital information.

Hardware[4] that may be used for gathering and analysing digital information includes:

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

- 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;
- Mobile Device Analysis Tools – used to read content on device as well as 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 destination 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 competition agency's 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; and
- Hardware Write Blockers – used to ensure that digital information is not changed during the review and acquiring process.

7.2 Dedicated computer forensic areas

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

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

7.3 Practices and Procedures

It is good practice to develop internal policies and procedures with regard to the collection and analysis of digital evidence.

Respecting internal policies and procedures with regard to the collection and analysis of digital evidence will assist in ensuring that the use of digital evidence in an investigation can withstand challenge in a court of law or other legal context. Also, such policies and procedures provide an assurance to staff as to what is expected from them whilst at the same time ensures that the competition agency has anticipated possible and foreseeable challenges that may arise with respect to the digital evidence.

7.3.1 General

Policies 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 competition agency's own forensic specialists; and
- Quality by reviewing standard operating procedures.

7.3.2 Preparation

<u>7.3.2.1 Searches, Raids and Inspections</u>

Pre-search, raid or inspection intelligence:

The following actions regarding pre-search, raid or inspection can be considered:

- 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(s);
- Seek available information about the companies' used cloud computing, including web-based e-mail and offsite data storage;
- Provide officers with technical information related to the collection of digital evidence;
- Use anonymous web access for internet inquiries of company information. This will not leave traces that may alert the suspected companies of an impending search, raid or inspection; and
- Consider an "Electronic Evidence Case Plan" early in the case to focus on the identification, preservation and collection of digital evidence. The plan will focus on what types of digital evidence may be used, where it is located or stored, how many places it may be found, etc. These issues will affect the timing of any search, raid or inspection and maximize the seizure of digital evidence.

Physical preparation:

- Ensure that all media to be used are forensically wiped/cleansed and formatted;
- Ensure that all software to be used is updated;
- Ensure that all hardware to be used is validated and functioning properly; and
- 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:

- Provide information to search teams about (new) technologies and devices which store digital evidence that may be found at a search, raid or inspection premises (*e.g.* iPods, memory cards, WiFi hard discs and other wireless devices, smart phones, USB devices, etc.);

- Provide advice to the search teams as to the correct handling of electronic media and digital information located at the search site;

- Discuss with the lead officer the search strategy to be used;

- Provide the search 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, raid or inspection with regard to the digital information;

- Specify the digital information to be collected, including keywords for search;

- Specify the names of persons who are targets, including key e-mail accounts;

- Have forensic specialists targeting computer systems; and

- Preserve digital information before any search begins to avoid destruction or alteration. For example, the G8 24/7 Network[5] provides an avenue to request the preservation of electronic evidence in other countries pending legal process.

7.3.2.2 Compelled Production

The following actions can be considered:

- 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 information; and

- Give instructions on how companies must produce digital information 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 evidence 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

[5] Some background information on the 24/7 Network is available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/presentations/Regional%20Ws%20on%20Cybercrime_13 May10/2215_The_G8_24/7%20Network_SStaro.pdf; http://www.oas.org/juridico/english/cyb20_network_en.pdf and http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

information, in order for the digital evidence to be legally admissible. The following are examples of methods used by some, but not all, competition agencies to ensure and demonstrate the authenticity of the digital evidence:

- 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 numbers or printable digital media discs;
- Describe possession of data, equipment, data carriers etc.;
- Make forensically sound bit stream copies;
- Use dedicated forms for documentation;
- Have written statements of the company to declare the seized digital information is in its original state; and
- Have written statements of the company to declare that they have received a copy of all the copied data and the hash value of the file.

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, competition 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 company and the competition 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 and document media to be taken from the premises;
- 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;
- Label all handled materials; and
- Record serial numbers for computer media, where available.

7.3.5 Gathering

It is good practice to establish control of the company's digital information as soon as possible after entering the premises in order to prevent its destruction.
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 competition agencies must return non-relevant digital information to the company, while other competition 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 production in certain circumstances.

- Supervise the company's system administrator during the entire process;
- Preserve digital information as originally acquired;
- Have a prepared a policy about bringing down servers;
- Do not switch on hardware that is switched off;
- Describe the location of all machines and data carriers;
- Identify external devices;
- 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;
- Record date and time of computer settings;

- Find and gain cooperation of the company's 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 digital information for the company;

- Look for the presence of "wipe software". This may also be part of the analysis of the digital information;

- 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; and

- Obtain the Service Agreement that the company may have concluded with an outside IT service provider and ensure that the company uses its contractual rights to assist the competition agency, if and when needed.

Some competition agencies perform live forensics during on-the-spot searches, raids or investigations. One competition agency stated that this has the advantage of less processing and analysing at the competition agency's office. However, another competition 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 the hard copy search will not be available at that stage, limiting the effectiveness of any keyword search.

7.3.6 Preservation of Digital Evidence

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

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

7.3.6.1 Searches, Raids and Inspections

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

- When entering the premises, do not turn off devices. By leaving a device on, forensic specialists may recover passwords to programs or other encrypted data that may be stored in memory or RAM. Other information in RAM may include identification of

network connections and internet activity. Once the device is turned off, the options to recover encrypted data become limited;

- Remove computer users from keyboards of computers that are identified as key search priorities and collect and control portable data carriers until such time as they have been examined;

- Record user attribution evidence (to identify who the user is if later contested and whether others may be logged onto the computer);

- Request a company official to direct company employees not to impede the inquiry by deleting, destroying or removing any records (including digital records) from the premises. If the destruction of digital evidence constitutes an offence that can lead to criminal and/or administrative sanctions, be sure to convey this fact to the company's employees;

- During the initial seizure, new leads may be identified such as data maintained on the cloud or other accounts which may need to be preserved or followed;

- Mailboxes may be locked at the server level, equipment (PC, laptop, floppies, CDs) may be locked in a secure and sealed place until examination or server backup media may be seized during the investigation; and

- Ensure that no unauthorised person has access to any electronic devices at a search site; unplug network cables from the computers; take care to ensure that storage devices are protected from static electricity and magnetic fields; and pack all digital information in antistatic packing in a manner that will prevent it from being bent, scratched, or otherwise deformed.

7.3.6.2 Compelled Production

Some competition agencies require 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 competition agency or investigative staff. Other competition agencies make copies of electronic media (*e.g.* CD-ROMs) containing the digital information as soon as it has been received by the competition 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 handles only the "working copies" of the media (*i.e.* a duplicate CD-ROM).

7.3.7 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 and/or all appeals are exhausted.

Processing may include the 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 (*i.e.* made at the premises during a search, raid or inspection) need processing afterwards. In general, copies of individual files and folders, like in compelled production, need less processing. Processing of data means to make available and/or visible the collected digital information for investigating purposes.

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

7.3.8 Analysing

The most used method for the analysis of digital information is keyword searching to find relevant documents. With the constant change of technology, however, this may 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; and
- Use information from analysis of the hard copy documents collected during the search, raid or inspection.

The following are other analytical options mentioned:

- Review all digital information;
- Confirm user attribution;
- View the print spoolers;

- Test file signatures looking for bad file 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 electronic documents;
- Look for connecting documents;
- Use search strings, code words; and
- Use intelligence software to provide link analysis.

Forensic specialists report to officers about the relevant digital information, including whether there are gaps in information, such as extremely few or no 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 digital gathering process.

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

7.3.9 Storing information after case closure

After case closure it is of vital interest to the subjects of the investigation to learn what happens to the digital information gathered during searches,raids and inspections. One competition 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 competition 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 competition agencies are required to store the information gathered or a copy thereof either permanently or temporarily. Sometimes only hard copies are kept whereas, in other cases the data itself is filed.

Some competition agencies keep the "original" images until the end of the legal proceedings. Therefore, the non-relevant electronic documents are deleted from the working copy when the

investigation phase is finished. The non-relevant electronic documents remain at the competition agency on the original images, however, access to them is strictly limited.

8 CHALLENGES CONCERNING DIGITAL EVIDENCE GATHERING

8.1 General

It is good practice to be cautious in drafting the scope and wording of terms in legal orders.

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

Legal issues mainly concern the authority of the competition agency to retrieve digital information from the company. This is of course an issue strongly related to the powers of the competition agencies governed by 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 surrounding digital evidence gathering. 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 competition agencies. In some cases, competition agencies may have written guidelines as to how to deal with these issues.

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

With digital information becoming more significant and gathering increased attention, case law is developing on all of these issues

8.2 Power for digital evidence gathering

Typically, national law gives competition agencies the power to perform digital evidence gathering, either by way of searches, raids or inspection or by way of compelled production. In almost all jurisdictions, this power is interpreted from an already existing power to compel or seize documents relevant to an on-going investigation.

As technical developments are rapid, the fact that many jurisdictions derive their power from an interpretation of already existing powers appears to be 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 electronic documents may emerge. Further, it is important for competition agencies to ensure that the legal authority to search and seize digital evidence

includes the ability to search and seize evidence concerning the use and control of the computer or device.

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 competition 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 competition agencies. In the case of hard-copy documents, there exist common ways to ensure that these documents are not seized or copied by the competition 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 electronic documents cannot always be studied or looked into at the company's premises. The data carrier on which the digital information is stored will often be imaged and further examined at the office of the competition 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. Competition agencies that are not allowed to seize or copy legally privileged or private documents will first try to extract the legally privileged or private documents from the data carrier and then make a digital copy of the data carrier. For instance, if digital copies are made at the premises of smaller stand alone data carriers (*e.g.* 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. In some jurisdictions, the competition 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 competition agency. In other jurisdictions, if a claim of privilege is made, the agency is forbidden to examine the documents over which the claim is made and the document or the data carrier must be sealed. The court will ultimately decide whether privilege attaches to the document.

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 digital copies of larger data carriers, it may be impossible to remove all privileged or private digital information at the premises of the company. This may restrict some competition agencies in their ability to image bigger data carriers.

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 competition agency's office. Otherwise, the stay on the site would be prolonged and may be unnecessarily disruptive for the company being searched, raided or inspected. The analysis is done in various ways. At some

competition agencies, before looking at the content of the digital information - as in the case of an image - a company and its lawyer will be invited to the competition agency's office to come forward with the names of the electronic 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. Digital information that is legally privileged or private is then destroyed or returned to the company. The remaining digital information on the copy will be analysed and studied by the competition agency. In case of disagreement, a formal protest can be made or the company can go to court to fight the judgement of the competition agency.

Some jurisdictions have a special provision in their law to deal with claims of legal privilege. In these jurisdictions, the digital information which the company claims legal privilege may be copied to separate media and sealed pending an agreement being reached about the claim between the lawyers of the company and the competition agencies. Sometimes an independent third party, or even the court, will decide the claims. Such an independent third party may consist of personnel from another location of the competition 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 hard copy information, one of the legal issues is whether competition agencies have access to and can seize digital information stored on a server outside the business premises.

Three different situations can be distinguished:

- a situation in which the server is not located at the specific premises of the company being searched, raided or inspected, but at another premises of the company;

- a situation in which the server is not located at the premises of the company being searched, raided or inspected, but at the premises of another company contracted for this storage (third party); and

- a situation in which the server is located outside of the territorial jurisdiction of competition agency.

There are two general approaches:

Some competition agencies look at whether the company searched, raided or inspected has access to and/or uses and/or controls the digital information stored at the other business premise(s) of the company. If the company has access, uses and controls such 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 therefore of no issue. This approach can be called "the Access approach".

Other competition 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 (*e.g.* search warrant, court order, administrative decision, etc.) the competition agency must get a new legal order to obtain access and be permitted to copy the digital information at the alternate location.

Therefore, some competition 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 company’s inspected premises

8.4.1.1 Another premises of the same company

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

In the Location approach, the competition 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 during the course of the search, raid or inspection.

8.4.1.2 Premises of another company

In the Access approach, if the company searched, raided or inspected has access to and/or uses and/or controls the digital information at the premises of another company, the digital information is considered to be accessible at the searched, raided or inspected premise(s) and access is allowed.

In the Location approach, the competition agency will need a new legal order to get access to the digital information regarding the premises of another company, 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). As noted above, for the Location approach, as new leads are identified (such as data stored on a cloud or new accounts), it is recommended that steps be taken to preserve the digital evidence (such as through the 24/7 Network referenced in Section 7.3.2.1) pending legal process.

8.4.1.3 Digital information stored outside the territorial jurisdiction of the competition agency

If the competition agency follows the Access approach, when the company that is being searched, raided or inspected has access to and/or uses and/or controls the digital information, the competition agency has, through the searched, raided or inspected premises, access to the digital information in the other territorial jurisdiction.

Competition agencies that follow the Location approach will not be allowed to access the digital information stored outside the territorial jurisdiction. Additionally, the Location approach will also prove to be insufficient in cases of cloud storing where data is stored on servers in unknown locations on the internet. In these cases the competition agencies use the possibility of mutual legal assistance treaties (MLATs) or agreements to gather the digital information.

8.5 Using digital evidence in court

Competition agencies may introduce the digital information gathered in different ways during the course of the investigation and at trial. There appear to be no significant legal problems in using the digital evidence gathered in court, providing procedures are properly followed.

8.6 Collecting data from third parties / cloud computing

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 competition agencies may require a new legal order (this may also be due to the fact that this kind of data may not be physically stored at the company searched, raided or inspected). With regard to the collection process as such many competition agencies reported that the process of collecting (*i.e.* the copying of data) does not differ from collecting data from the companies inspected.

8.7 Bring Your Own Device

Many companies have policies that allow employees to use their own electronic devices, such as personal computers or smart phones, for work purposes. Often, these devices will contain a combination of personal and professional information. As a result, it is important to be cognisant of these types of policies when drafting legal orders and preparing for searches, raids or inspections.

8.8 Information to Provide to a Company

When conducting searches, raids or inspections, it is important to consider what information competition agencies should provide to the companies they are searching about the investigation. On the one hand, supplying a company that is being searched, raided or inspected with comprehensive information regarding the investigation would permit the company to assist the competition agency in ensuring that the digital evidence gathering process is as targeted and thorough as possible. On the other hand, competition agencies may have concerns that providing detailed information to a company may result in the deletion or destruction of evidence, or the tainting of witnesses. Competition agencies should consider these factors when deciding how much information to provide to companies being searched, raided or inspected.

8.9 Transparency of a competition agency's procedures and workflow

In a similar vein, it is also important to consider to what degree a competition agency should be transparent with respect to its procedures and workflow for digital evidence gathering. Having a high level of transparency will help to ensure that a competition agency remains consistent and fair with respect to its digital evidence gathering procedures. However, a high level of transparency can cause problems for competition agencies in situations where, for whatever reason, they did not follow their published procedure. This may be of particular concern in cases that are brought to court. Conversely, being less transparent about

procedures and workflow allows competition agencies to be more flexible in the digital evidence gathering process; though they may still be open to scrutiny due to the secretive nature of their procedures. Again, competition agencies should consider these factors when determining the level of transparency of their procedures and workflow for digital evidence gathering.

9 Advantages and Future Challenges

Most competition agencies indicated that digital evidence gathering was advantageous for getting access to significant information. A number of competition 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 competition agency reported that the main advantage is that information about the company's competitive strategy and communication between the competitors are usually found on digital media.

- One competition agency reported that the main advantage with making forensic images is the possibility to restore erased data. This enables the competition agency to collect evidence of an infringement even if the search, raid or inspection was expected and the company has been "cleaning up".

- One competition agency reported as an advantage that extra time and resources were granted by post-inspection analysis.

Some examples of challenges:

- Some competition agencies advised that digital evidence gathering contains challenges as the competition agencies have to keep up with the companies' rapid advances in technology.

- One competition agency warned that keyword searches can be thwarted through the use of code words or intentional misspellings.

- Some competition agencies mention the lack of sufficient resources (*e.g.* IT staff, hardware, software, licensing and training) as a challenge to be overcome in the future.

APPENDIX 1: GOOD PRACTICES RELATING TO DIGITAL EVIDENCE GATHERING[6]

The following list reflects good (?) practices common to many of the competition agencies responding to the November 2009 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 IT staff/forensic specialists to work closely with the case handlers during all stages in the gathering of digital evidence.
- to give special training to the competition agency's staff who collect and process digital evidence.
- to describe the scope and nature of cooperation with other public agencies in a protocol on digital evidence gathering.
- to have a dedicated budget to cover the costs of purchasing and maintaining hardware, software, licensing and forensic tools, as well as staff training.

The Elements of Digital Evidence Gathering

It is good practice:

- to use tools that are thoroughly tested and generally accepted in the computer forensics field.
- to develop internal policies and procedures with regard to the collection and analysis of digital evidence.
- to document every step taken in the digital evidence gathering process.
- to establish control of the company's digital information as soon as possible after entering the premises in order to prevent its destruction.
- to seek the company's systems administrator's cooperation as the administrator is generally an important person with regard to digital evidence gathering.

[6] Please note that good practices set out in other Chapters of the *Anti-Cartel Enforcement Manual* may also apply to this Chapter.

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

- to determine user attribution early during each phase (such as during the initial search and seizure and during the examination).

- to have digital evidence gathering practices and procedures that inhibit and help prevent 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 and/or all appeals are exhausted.

Legal issues concerning Digital Evidence Gathering

It is good practice:

- to be cautious in drafting the scope and wording of terms in legal orders.

- to keep in mind the principle of integrity and authenticity of digital evidence during the entire legal 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: EXAMPLE CO-OPERATION PROTOCOL

Section 1: “The purpose of the agreement is to secure a human resource mass that can provide mutual assistance on digital evidence gathering, that can provide technical equipment for mutual loan, that can provide a continuous methodological development in gathering and handling electronic evidence and that can maintain and develop the staff skills on Forensic IT.”

Section 2: “Type of cooperation – assistance for digital evidence gathering. The agreement covers only technical assistance to the digital evidence gathering for the competition agency’s inspections, and the staff act solely of the basis of the law of the requesting competition agency and is subject to the powers and the instructions of this competition agency. The agreement does not cover assistance to processing and assessment of the evidence of the secured data.”

Section 3: “The staff must have the skills to individually perform digital evidence gathering according to the standards described in Section 4. Staff under the tutelage must not perform digital evidence gathering on their own. The competition agencies keep a common list of staff skill level, education level and certifications.”

Section 4: “The requesting competition agency determines the standards and the methodology on digital evidence gathering for the specific inspection, but electronic data always has to be gathered without causing changes to the IT environment of the involved target companies, and so that the secured data can be used as evidence in court. Furthermore there must not be any doubt of the origin and the authenticity of the data, and the secured data must be identical to the data that was located in the IT environment of the involved target companies at the time of the inspection. Electronic data must be gathered by the use of licensed forensic hardware and software of the competition agencies. The data has to be secured to special hard drives, and the staff has to make sure, that the data that has been selected in the IT environment of the target companies, is transferred and stored to the hard drives before leaving the companies.”

Section 5: “The requesting competition agency determines the demands for documentation and report writing on the performed digital evidence gathering jobs.”