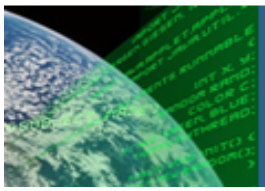

GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

www.coe.int/cybercrime

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Strasbourg, France

Draft Version 29th January 2018

Cybercrime Benchbook for

Judges and Magistrates

and

Cybercrime Guidelines for Prosecutors

Version 2018

DRAFT v.3

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contact:

Data Protection and Cybercrime Division

Directorate General of Human Rights and Rule of Law

Council of Europe,

Strasbourg, France

Tel: +33-3-9021-4506

Fax: +33-3-9021-5650

Email: alexander.seger@coe.int

Disclaimer:

Contents

1. Introduction

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities.

The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society.

GLACY+ (Global Action on Cybercrime Extended) is a Joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe. GLACY+ is intended to extend the experience of the GLACY project (2013 – 2016) with the objective to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

In this framework, three objectives have been defined:

1. To promote consistent cybercrime and cybersecurity policies and strategies.

2. To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.

3. To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.

Under Objective 3, the GLACY+ project will work toward ensuring that judicial training academies are providing training on cybercrime and electronic evidence as part of their regular curricula.

In this context, also building on the results coming from the initial assessments conducted in the Priority/ Hub countries, as well as the previous work accomplished on similar topics within the iPROCEEDS Project, the GLACY+ Project organized the following activities:

• Update of the introductory training of trainers (ToT) modules on cybercrime and electronic evidence for judges and prosecutors, to make it suitable for delivery in countries with diverse legislative frameworks (e.g. Common Law/ Civil Law).

• Definition of a new concept for the advanced training modules on cybercrime and electronic evidence for judges and prosecutors and realization of the supporting materials.

• Creation of a bench book on cybercrime and electronic evidence for judges and prosecutors.

This Bench book for Judges and Magistrates and Guidelines for Prosecutors on cybercrime and electronic evidence should provide members of the judiciary and prosecution first and basic support about cybercrime issues connected to their cases. In the first place it should provide basic explanation for number of the computer and cybercrime related terms and meanings in the form of the glossary.

Additionally, judges and prosecutors will be able to have a close insight into the case law of different countries within the field of cybercrime. Coming from Prosecution or Court cases, experiences presented in the appendix of this Benchbook (Guidelines), should provide additional value to the considerations starting from the very first steps of the criminal investigation, being it led by police or more contemporary led by Prosecution, to the final stages of first and final instance adjudications in Courts.

In this first itteration of the Benchbook (Guidelines), only limited number of these cases are presented for Prosecutors and Judges consideration as a reference. Still, included cases are covering most contemporary threaths of the cybercriminality and their outcomes, taking into account not only the successful cases but also dropped or abolished cases with closer insight and reasonings of such outcomes.

GLACY+ Project will continue during its implementation to update this Benchbook (Guidelines) with additional examples coming from various countries and legal practices, being that Common Law, Civil Law or hybrid systems.

Last but not least is appendix connected to the Electronic Evidence Guide of the Council of Europe, which was originally prepared under the joint regional project Cybercrime@IPA of the European Union and the Council of Europe (COE) on cooperation against cybercrime under the Instrument of Pre-Accession (IPA).

The first edition was published on 18th March 2013 and has since become a popular resource for law enforcement and judicial bodies in a variety of different countries. Some countries have even translated the guide into their domestic languages. The second edition of the Guide is the current basis for materials used in this document and based on the feedback provided by readers.

2. Substantive Law

Section 1 of Chapter II of the Convention (substantive law issues) covers both criminalization provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions.

The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

2.1 About Definitions

A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

2.2 About Service provider

The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems (cf. also comments on Section 2). Under (i) of the definition, it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a

fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network.

Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (i). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (i). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services.

2.3 About Traffic data

For the purposes of this Convention traffic data as defined in article 1, under subparagraph d., is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself.

In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.

The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity.

2.4 About Illegal access (Article 2)

"Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data).

"Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organization. The act must also be committed 'without right'.

There is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."

Case law example:

To be added.

2.5 About Illegal interception (Article 3)

The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons.

The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices

Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted.

For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right".

Case law example:

To be added.

2.6 About Data interference (Article 4)

The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

'Damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognizable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person

who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

The above acts are only punishable if committed "without right". In addition, the offender must have acted "intentionally".

Case law example:

Creating and Introducing of Computer Viruses

The verdict stated that the defendant using Visual Basic program on his personal computer created Trojan computer virus with the intent to introduce it into another's computer in order to capture pictures of active screen of the infected computer (Screenlogger) and to monitor each keystroke a user types on a specific computer's keyboard (Keylogger); he uploaded and downloaded content to and from infected computers. The defendant also formed two chat rooms which he used for issuing commands and monitoring infected computers. He introduced the virus into computers of 70 users causing damage to the computers and their users by recording everything their computer monitors displayed on the screen, recording everything the users typed on their keyboards and then without users' knowledge sending these information to a server under his control. This was done in such a way that firstly he sent e-mails under false names from different e-mail addresses to the addresses of users. E-mails contained infected attachment after whose opening the virus was installed into computers, copied into program register, and then made system recordings which then enabled activation of the virus with each activation of the operating system.

Similar example of this criminal offence is of a defendant who created and introduced a virus into computers of others and then sent commands to the virus via text messages and collected personal, business and other data of the users of infected computers. In this way he introduced the virus into computers of three German citizens, obtained data on their bank accounts for online transactions and then with the intent to illegally acquire material gain, by false presenting of facts he misled one of those German citizens and a German bank officer in order to get them to pay € 2,600 at the expense of their client's assets.

The defendant managed to acquire this German citizen's data: name and surname, landline phone number and mobile phone number, bank account number, user name, PIN (personal identification number which is a numeric code for identification of the user), TAN number (transaction authentication number which is a one-time numeric code) used for verification of transaction.

Besides, the defendant misled the same German citizen by giving him false information that he had gotten amount of € 1,300 as a gift from his bank. He did this by creating a false bank website using HTML in appropriate web editing software. The web page was in German language with the text

confirming that this German citizen was awarded € 1,300 for successful business i.e. for trading securities.

The web page prepared in this manner was introduced into the hard drive of his computer. When this German citizen logged in to check up his bank account, the defendant activated Keylogger in order to monitor data entry; he recorded the number for online transactions and misled a bank officer to make a payment to the defendant's mother's bank account with the false purpose of payment. The bank stopped this payment as its checking showed that it might be a high-risk transaction.

In his statement the defendant gave detailed explanations which were of great importance both for the first and second instance courts so they could perceive the way of commission of criminal offences that not many judges had previously encountered.

In the evidentiary hearing procedure an official letter was read that a domestic bank had received from the injured party's country CERT (*computer emergency response team*) from which it was determined that the virus in question was Trojan with its description – what are its functions, what are the functions of the introduced content to the infected computer, how it receives commands, from where and how it was controlled and response from the infected computers. In the evidentiary hearing, inspection of the hard disk drive was performed using forensic software tools. Activation of the data was performed using Forensic toolkit, and it was established that the computer was used for access to the Internet and for other purpose, and certain files were found and submitted to the court on CD-R.

The content of the submitted discs was examined in the court and it was determined that on the laptop's hard drive of the defendant among other data there were screenshots of the injured party's computer with his bank account data on it etc.

First instance court found that the consequence of the criminal offence Creating and Introducing of Computer Viruses is causing damage but unlike the defendant and his attorney's interpretation, the court found that damage can be manifested in any form and not only in sense of material damage, but it is enough that the introduction of the virus had such consequences as "slowdown in the work of the computer, system crash or its shutting down and restarting every few minutes, slowdown of the Internet connection and the like". Damage can also be observed as non-material, considering the fact that the right to privacy and the protection of confidential data of users of infected computers was violated.

This particular case was the criminal offence of attempt of fraud. The first instance court found that the defendant used computer, computer programs and the Internet in his commission of the criminal offence which in the opinion of the court are the means suitable for commission of the criminal offence in question.

Regarding the evidence, it is necessary to determine if the computer virus was introduced with the direct access to computer or it was done within an internal network using other computer which was the part of that network or it was done via internet. Perpetrators of this criminal offence are usually persons whose knowledge significantly exceeds basic computer knowledge and who understand how operating system works, functioning of separate units and their mutual interactions, they know how to make computer programs with some of the existing program languages and tools.

2.7 About System interference (Article 5)

The provision aims at criminalizing the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly.

The term "hindering" refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.

The hindering must furthermore be "serious" in order to give rise to criminal sanction.

The hindering must be "without right".

The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

Case law example:

See next page "About Misuse of device (Article 6)"

Computer Sabotage

The defendant was on the position of the chief analyst for Information and reporting in a company, and he deleted computer data from a computer he was responsible for and which was situated in the official premises with the intent to prevent or significantly interfere the electronic processing and transmission of data process which are of importance for his service. He deleted over 5,000 documents that were marked as "official secret" or "for internal use".

At the trial there was an expert witness, IT engineer by profession who explained the procedure of making a copy of a hard disc. He explained that by usual deletion data are not permanently removed from the computer but only the information that the data existed on it, so the data were restored from the hard disc image. They generated imprint of SHA256 (Secure Hash Algorithm) and determined the time of data deletion.

An example of good practice: It is stated that the expert witness invited the responsible person, a head of department who was present at all times during the expert evidence, that the report was made, that prior to expert evidence the computer was sealed, that the deletion in the case in question was performed by simple deletion, therefore the hard drive was not formatted.

The expert witness further explains what actually happens if a disk is formatted – in that case all the files contained on the hard drive are permanently deleted, even the operating system. In this case it was found that the deleted documents from several folders had the extensions .doc and .exl i.e. Excel spreadsheets and Word documents. The expert witness refuted defence's claim by explaining that it was not the virus that led to the deletion of the folders, because not all the documents with specified extensions were deleted.

The report on the expert evidence of MoI's Special investigative methods service, the Department for the collection and processing of digital data was read, which explained how the activation of the data was carried out and what was found in the computer. Computer forensics software was used and the contents of the hard disk were fixed by generating digital fingerprints SHA 256. All this was recorded on a disc that was submitted to the court and its content was examined at the trial. The first instance court concluded that the findings and opinion given by the expert witness who is qualified in the area of expertise are logically derived from the facts.

2.8 About Misuse of device (Article 6)

Perpetration of this act includes the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data.

In its different national iterations act should nevertheless criminalize the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the cybercrime offences.

Term 'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

Act should criminalize the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

Also possessing of such items should create this offence. The offence requires that it be committed intentionally and without right. Authorized testing or the protections of a computer system are not covered by the provision.

Case law example:

Unauthorised Access to Computer, Computer Network or Electronic Data Processing, Computer Sabotage, Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data and Creating and Introducing of Computer Viruses

One of the interesting cases in which the final verdict was rendered was the criminal proceedings against the defendant who was found guilty on five counts: on the first count of the criminal offence of Unauthorised Access to Computer, Computer Network or Electronic Data Processing, of the criminal offence of Computer Sabotage, of the criminal offence Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data; on second, third and fourth count of Unauthorised Access to Computer, Computer Network or Electronic Data Processing, and of Computer Sabotage; and on the fifth count of prolonged Creating and Introducing of Computer Viruses, and prolonged criminal offence of Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data.

Violating protective measures, the defendant without authorization logged in to a computer network, accessed electronic data processing in such a way that he had previously used anonymous service providers such as hotspot or wireless which provide access to Internet through open wireless access points to change MAC addresses (Media Access Control Address) of the Network Interface Cards of the computers that he had used, using several Socks5 connection protocols (Internet protocol that directs network packets between client and server via the proxy server and provides authentication so that only authorized users can access the server, which enables the IP (internet protocol) address to be concealed, i.e. that communication with another computer goes over a remote computer (server) for serving other computers that randomly assign IP addresses from any range of addresses, keeping the true IP address unrevealed).

Then, without authorisation he accessed to a protected computer network, a central server for control of web sites of a company for providing services of accessing the internet on whose server a web site of a state authority was hosted. Then, using his alias he entered, destroyed, erased and changed and thus made unusable computer data and programs, with the intent to disable and obstruct the process of electronic data processing which is of importance to the said state authority. He did this in such a way that in the electronic record of the central control server he deleted the so-called administrative user access data (user administrative name and password to unlock/provide access to editing of the website) to disable further access by authorized persons to data control and the website itself. Then,

he changed the username and password entering so-called "standard values" for the name and password which in this particular case were admin-admin, and after that he gave the data for use to other in order to commit the offence of Unauthorised Access to Computer, Computer Network or Electronic Data Processing, in such a way that he immediately distributed the said data through a variety of social and communication networks on the Internet to other persons, for continued unauthorized access and changes to the content of the said website.

We chose this example as it clearly demonstrates that it is necessary that the judges and prosecutors apart from their undoubtedly existing knowledge from the procedural and substantive criminal law also master the basic forms of cybercrime.

Second count charged the defendant with almost identical way of commission of the criminal offence, and the only difference was that the defendant had accessed the central server for control of all websites of internet service providers, on whose servers there were websites of different state authorities, public services, companies and other subjects. The defendant entered, destroyed, erased and changed and thus made unusable computer data by changing user access data, and then in the electronic database of websites he changed the texts and photos and other electronic data or completely erased websites and information and instead of them he entered previously prepared his own presentations with various messages into publicly available electronic databases thus accessing without authorisation and preventing or significantly interfering with the process of electronic processing and transmission of data on internet sites of several faculties and courts at different levels among others, and then accessed the websites of the various political parties, media agencies, ministries, the site for the parliamentary elections and others.

On the count five the defendant was found guilty for having made a computer virus with the intent to introduce it into others' computers and computer networks. On his personal computer the defendant had made a computer virus and then published it on a number of hacker internet websites. When a user would take it over and use it, it would return to the defendant in the form of the new PHP Shell (which is used for administration and maintaining websites, for unpacking and moving large files) with the information where the virus is situated and exactly in which way an infected computer can be controlled. On one of his e-mail addresses he had 600,000 Shells obtained in this way, and on the other 176,000 Shells. One Shell served for access to one website, so the defendant had access to each infected computer used by another person who didn't even know that their computer was infected which enabled the perpetrator to access other websites on the servers via so-called "backdoor" approach. He then entered those 776,000 PHP Shells in others' computers and computer networks on the websites that he had changed and by doing so caused damage by disabling access to and use of those websites in the way they were made, and thus at the same time caused material damage in an undetermined amount.

What is particularly interesting is that the defendant who was a high school student (unmarried, no children) confessed committing of all the criminal offences he was charged with (there were twelve) and that he committed them over a one year period.

In its integral version his defence had 6 pages. We can get the picture from his defence how young people think, what motivates them and why they commit such criminal offences. Also, the court can understand how easy it can be for a perpetrator to perform actions that have all elements of criminal offence in the area of cybercrime.

In finding evidence it is important to get a report from the Internet provider which hosted each web page on access logs on server as well as the contents of the websites before and after they were attacked.

2.9 About Computer related forgery (Article 7)

The purpose of this article should be to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data.

Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.

This provision covers data which is the equivalent of a public or private document, which has legal effects. The unauthorised "input" of correct or incorrect data brings about a situation that corresponds to the making of a false document. Subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document. The term "for legal purposes" refers also to legal transactions and documents which are legally relevant.

Act requires in addition an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Case law example:

To be added.

2.10 About computer related fraud (Article 8)

To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' are supplemented by the general act of 'interference with the

functioning of a computer programme or system'. The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles. Article should cover acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

The computer fraud manipulations are criminalised if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person. The term 'loss of property', being a broad notion, includes loss of money, tangibles and intangibles with an economic value.

The offence must be committed "without right", and the economic benefit must be obtained without right.

The offence has to be committed "intentionally".

Case law example:

Defendant in this case was charged with misleading citizens by false presentation of facts and leading them to make payments in the amount that exceeded certain amount in total in such a way that he registered a domain with the web site under the title "Appeal for help" where he introduced himself as a father of an ill 18 month old boy who needed urgent medical intervention i.e. stem cell transplant which was allegedly scheduled in a hospital abroad and which costed € 145,000.00. He posted more than hundred photographs of an unidentified child with its parents claiming that it was his ill child and asking all the people who wanted to help him to make payments on his two bank accounts. He then contacted the website administrator again falsely introducing himself and asked them to post the same appeal on the websites they administered, which they did, and then on his domain he posted the list of websites that supported the action, after what he got payments from a number of people and he withdrew the money from his accounts.

In the evidentiary procedure provider's reports were read which showed that the defendant had paid for the registration of the domain for three-months hosting, that he had created a domain and time and place of that action, there were his data, telephone numbers and e-mail addresses that he filled in the registration forms; that on the same day he started his website from an IP address belonging to TelCo operator. From the Internet provider report it is also determined that two connections were recorded to the e-mail accounts which belonged to the defendant from the IP address assigned to the user i.e. the defendant. These connections were realized via ADSL installed on a landline with the same telephone number that the defendant filled in the registration of domain form. It was the telephone connection whose subscriber was the defendant's mother while ADSL was registered on the name of the defendant.

2.11 About Child pornography (Article 9)

Article seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.

This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. It criminalises the production of child pornography for the purpose of distribution through a computer system. It also criminalises the 'offering' of child pornography through a computer system. 'Offering' is intended to cover soliciting others to obtain child pornography. 'Making available' is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography sites.

Provision should also criminalise the distribution or transmission of child pornography through a computer system. 'Distribution' is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of 'transmitting' child pornography.

The term 'procuring for oneself or for another' means actively obtaining child pornography, e.g. by downloading it. The possession of child pornography in a computer system or on a data carrier, such as a USB drive or CD-Rom, is criminalized.

The term 'pornographic material' is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt.

A 'sexually explicit conduct' covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It should not be relevant whether the conduct depicted is real or simulated.

The three types of material defined for the purposes of committing the offences represent depictions of sexual abuse of a real child, pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct, and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct

Provision should focus more directly on the protection against child abuse. It should aim at providing protection against behaviour that, while not necessarily creating harm to the 'child' depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse.

The term ‘without right’ does not exclude legal defences, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Provision must criminalise conduct if committed "intentionally."

Under some standards, a person is not liable unless he has intent to offer, make available, distribute, transmit, produce or possess child pornography. However, numerous jurisprudences adopted a more specific standard (see, for example, applicable European Community law in relation to service provider liability), in which case that standard would govern. For example, liability may be imposed if there is "knowledge and control" over the information which is transmitted or stored.

Case law example:

During their work police officers found out that an unknown person came into possession of photographs and audio-visual material of pornographic content that were produced by exploitation of children and juveniles for pornography.

Acting under orders of the investigative judge of the Higher Court the apartment and other premises at the address where the suspect has a permanent residence were searched, and the record on the search was made. During the search of the apartment and other premises, computer equipment used by the suspect, consisting of 4 hard discs and 27 DVDs were found and confiscated.

In executing the search of the apartment police officers had been refused entry to the apartment for more than 45 minutes as the mother of the suspect didn’t want to open the door claiming that her son was not at home. After they were allowed into the apartment, police officers found the suspect in the apartment. The equipment was confiscated and the receipt for the seized objects issued.

Also, during the search of the apartment, a hard disc that was thrown out was found on the ground under the window. Due to the prolonged time for entering the apartment and the nature of the search, there was a doubt that the thrown hard disc belonged to the suspect who had thrown it out prior to the entry of the police. Police officers executed investigation of the scene and confiscated the thrown hard disk and made an official note on it.

Acting under the stated order, in official premises of the police in the presence of the suspect, police officers conducted inspection and examined 4 temporarily seized computer hard disks, and determined that one hard drive (which was found in the room logged out of the computer) contained material produced by exploitation of children and juveniles for pornography. The size of the material was 865 MB.

Also, at the examination of the 2 hard disk drives that were in the computer case at the moment of the search, it was established that the primary hard disk was missing, i.e. the hard disk where the operating system is, as on the two hard disks in the computer case only the stored data were found.

Material produced by exploitation of juveniles for pornography was found during examination of the "Maxtor" hard drive with the capacity 80GB which was located in the C: partition of the computer, in the "Documents and Settings" folder, in the subfolder named "Bambi". There were 16 videos of total size 865MB.

Police filed criminal charges to Special Prosecution Office for High-Tech Crime against the suspect for the criminal offence of Showing, Procuring and Possession of Pornographic Material and Juvenile Pornography.

During the period from year 2008 until February 2013 using the "LimeWire" software which functions as a closed network, the defendant acquired and kept in his computer photographs and audio-visual material produced by exploitation of children and juveniles for pornography.

The record of the interrogation of the accused in the presence of his counsel was submitted as evidence to the criminal complaint. During interrogation the defendant stated that he had used the Internet for downloading pornography, that he hadn't consciously downloaded children pornography but that he had been downloading regular pornography using Torrent, Frostfire, LimeWire software, and that when choosing what he would download he would choose more material and let them download during night, and that he didn't watch all the material that he had downloaded. He also stated that when he came across children pornography he immediately erased it.

In February 2013, Special Prosecution filed a motion to undertake investigation in order to establish existence of elements of the criminal offence of Showing, Procuring and Possession of Pornographic Material and Juvenile Pornography. It was also asked that the accused was remanded in custody considering that the amount of the found photographs and audio-visual material produced by exploitation of juveniles for pornography, as well as the content of the material and the age of persons whose sexual abuse was shown in the material, indicated a risk that the defendant would repeat the criminal offence if he was released.

In February 2013 a motion was filed to the investigative judge of the Higher Court to undertake investigation, i.e. to issue an order for taking and analysing a swab of the defendants DNA, and also to examine the DNA evidence from the hard disk drive found on the spot, and to compare these two DNA profiles.

In March 2013, the National Criminal Technical Centre submitted their expertise opinion which shows that the DNA analysis of the biological trace samples taken from the hard drive contained a DNA profile that perfectly matches the DNA profile of the defendant.

In June 2013 a motion was filed to the investigative judge of the Higher Court to issue an order for extraction of digital evidence contained on the hard drive for which the expertise of the National

Criminal Technical Centre found that the biological trace that was found on it fully matched the DNA profile of the defendant MS.

The investigative judge of the Higher Court issued an order by which the expertise was entrusted with the private forensic company to perform extraction of digital evidence from the subject hard disk. The findings of the forensic company showed that the damage to the subject hard drive was such that it was impossible to perform the data rescue, reconstruction and forensic analysis.

In this particular case, the perpetrator of this crime is a 32 years old male, occupation: construction technician, unmarried, underwent civil military service, medium income, no prior convictions according to the report from the Criminal Record Office and there are no criminal charges against him for any other criminal offense.

In this particular case, the perpetrator of this crime had to have a computer with the Internet access and special programs installed which made possible exchange of files among the persons who had this software installed on their computers.

Specificity of this particular case lies in the fact that prior to the execution of the search by the police the perpetrator tried to destroy the evidence of the commission of this criminal offence by taking the hard drive out of the computer and throwing it out of the window. He did not completely succeeded in his intention as the pornographic material produced by exploitation and abuse of juveniles was found on another of his hard drives.

2.12 About offences related to infringements of copyright and related rights (Article 10)

Criminal act should criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale".

Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement

The obligation to criminalise infringements of copyright and related rights pursuant to obligations undertaken in international instruments does not extend to any moral rights conferred by the named instruments (such as in Article 6bis of the Bern Convention and in Article 5 of the WIPO Copyright Treaty).

The provisions are intended to provide for criminal sanctions against infringements 'on a commercial scale' and by means of a computer system.

However, specific provisions may go beyond the threshold of "commercial scale" and criminalise other types of copyright infringement as well.

Case law example:

Police department filed criminal charge against the suspect on suspicion of committing the criminal offence of Unauthorised Use of Copyrighted Work or other Work Protected by Similar Right.

Motion for investigation was filed to the Higher Court against the suspect on suspicion of committing the criminal offence of Unauthorised Use of Copyrighted Work or other Work Protected by Similar Right.

In the statement given before the investigative judge, defendant stated that police searched his apartment on which occasion police officers seized his computer with the monitor and printer and that during the search of his garage police found CDs with different films in DVD format, and that there were 796 pieces of compact discs with more than 4,000 different films on them.

The suspect stated that it was his private collection that he had never been selling or publicly screened, but that they were exclusively for his personal use. When asked about the fact that in his computer he had files containing film covers prepared for printing, the suspect stated that he had acquired those covers from various booklets and brochures which he later scanned and saved so that he could find out about the content of the films he had downloaded from the Internet.

After the investigation judge returned investigation files to the prosecution additional motion for investigation was filed which required that the police officers who executed the search of the defendant’s apartment and filed criminal charge be questioned as witnesses particularly if during the search they found empty CDs and if they did how many were there as this information was not stated in the receipt on seized objects.

After the investigation was concluded an indictment against was filed to the Higher Court for the criminal offence of Unauthorised Use of Copyrighted Work or other Work Protected by Similar Right as he was in the state of full mental competence and had the intent to put into circulation illegally multiplied copyrighted material i.e. optical discs with films in such a way that in his apartment and the garage he had 796 compact discs with total of 4,485 copyrighted works – films, and a number of files with films and film covers prepared for printing which were stored in his computer which had 4 DVD burners as well as a colour printer for printing film cover. The defendant was conscious of his act and its illegality.

After the hearing the Higher Court found the defendant guilty of the criminal offence he was charged with and was sentenced to 6 months imprisonment with the suspended sentence of two years in probation, during which time he is not to commit any new criminal offence. Additional safety measure imposed was seizure of objects under the Criminal Code.

The court did not accept the defence of the defendant that claimed it was his personal film collection, primarily on the grounds of testimony of witnesses - police officers who didn't have any reason to unjustifiably incriminate the defendant, and who stated that they were executing a search warrant of the apartment of the when they found a number of compact discs in the room next to the computer and larger number of CDs in the garage, all of them marked with numbers. These claims were documented with photographs. In the computer room there were a lot of empty CDs, a printer and several hard disk drives, as well as two boxes with about 50 empty CDs each. Given the testimony of the witnesses and the objects found and seized, it clearly follows that the defendant had the intent to acquire material gain.

Specificity of the case lies in the fact that the defendant was not charged with putting copyrighted material into circulation but only with keeping it with the intent to put into circulation. As the defendant did not have more than one copy of each film it made it difficult to prove his intents, and for this reason police officers who had searched the defendant's apartment and other premises were questioned regarding their direct findings and their testimony together with the material evidence in form of the receipt on seized objects and photographs showing that the seized computer had four DVD burners which implied multiple DVD burning convinced the court that the defendant was undoubtedly guilty of the criminal offence that he was charged with.

3. Procedural Law

The technological revolution, which encompasses the "electronic highway" where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. Equally, safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers.

One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.

All the provisions referred to in this Section aim at permitting the obtaining or collection of data for the purpose of specific criminal investigations or proceedings.

The procedures in general refer to all types of data, including three specific types of computer data (traffic data, content data and subscriber data), which may exist in two forms (stored or in the process of communication).

3.1 About Expedited preservation of stored computer data (Article 16)

Provision should be applied to stored data that has already been collected and retained by data-holders, such as service providers. It should not apply to the real-time collection and retention of future traffic data or to real-time access to the content of communications.

The measures described in the provision should operate only where computer data already exists and is currently being stored.

"Data preservation" must be distinguished from "data retention".

To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one’s possession into the future.

This provision refers only to data preservation, and not data retention.

It was required to introduce a power to order the preservation of specified computer data as a provisional measure, whereby data will be preserved for a period of time as long as necessary, up to a maximum of 90 days. A Party may provide for subsequent renewal of the order. This does not mean that the data is disclosed to law enforcement authorities at the time of preservation. For this to happen, an additional measure of disclosure or a search has to be ordered.

This will help to ensure that critical data is not lost during often time-consuming traditional mutual legal assistance procedures that enable the requested Party to actually obtain the data and disclose it to the requesting Party.

'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate.

Preservation does not necessarily mean that the data be 'frozen' (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users.

The power to order or similarly obtain the expeditious preservation of specified computer data applies to any type of stored computer data. This can include any type of data that is specified in the order to be preserved. It can include, for example, business, health, personal or other records.

The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor).

If provision gives effect to preservation by means of an order, the order to preserve is in relation to "specified stored computer data in the person's possession or control". Thus, the stored data may actually be in the possession of the person or it may be stored elsewhere but subject to the control of this person. The person who receives the order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure."

Order imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy.

Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure.

3.2 About Expedited preservation and partial disclosure of traffic data (Article 17)

This provision should establish specific obligations in relation to the preservation of traffic data and provide expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications.

Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system.

Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication.

Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted.

The competent authorities should specify clearly the type of traffic data that is required to be disclosed.

3.3 About Production order (Article 18)

Provision should enable competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications.

The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information.

Provision should enable competent law enforcement authorities to have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering jurisdiction territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering jurisdiction territory.

Provision shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". The term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control

"Subscriber information" in principle refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records.

Subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service.

The term 'technical provisions' includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks).

Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider.

It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement.

The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services.

The provision should not authorise issuing of a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

3.4 About Search and seizure of stored computer data (Article 19)

With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain. For example, the gathering of the data occurs during the period of the search and in respect of data that exists at that time. The preconditions for obtaining legal authority to undertake a search remain the same. The degree of belief required for obtaining legal authorisation to search is not any different whether the data is in tangible form or in electronic form. Likewise, the belief and the search are in respect of data that already exists and that will afford evidence of a specific offence.

Provision should empower law enforcement authorities to access and search computer data, which is contained either within a computer system or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or USB drive).

Provision should concern the search of a computer system and its related components that can be considered together as forming one distinct computer system (e.g., a PC together with a printer and related storage devices, or a local area network).

Although search and seizure of a "computer-data storage medium in which computer data may be stored" and may be undertaken by use of traditional search powers, often the execution of a computer search requires both the search of the computer system and any related computer-data storage medium (e.g., USB drives) in the immediate vicinity of the computer system.

'Search' means to seek, read, inspect or review data. It includes the notions of searching for data and searching of (examining) data. On the other hand, the word 'access' has a neutral meaning, but it reflects more accurately computer terminology. Both terms are used in order to marry the traditional concepts with modern terminology.

It allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'.

In certain cases, for instance when data is stored in unique operating systems such that it cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. This may also be necessary when the data carrier has to be examined in order to retrieve from it older data which was overwritten but which has, nevertheless, left traces on the data carrier.

As well as using the traditional term 'seize', if the term 'similarly secure' exists, it is included to reflect other means by which intangible data is removed, rendered inaccessible or its control is otherwise taken over in the computer environment.

The rendering inaccessible of data can include encrypting the data or otherwise technologically denying anyone access to that data. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography.

The term 'removal' is intended to express the idea that while the data is removed or rendered inaccessible, it is not destroyed, but continues to exist. The suspect is temporarily deprived of the data, but it can be returned following the outcome of the criminal investigation or proceedings.

Provision may introduce a coercive measure to facilitate the search and seizure of computer data. It can recognise that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision, therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.

The provision of this information, however, is restricted to that which is "reasonable".

3.5 About Real-time collection of computer data (Article 20)

Interception of telecommunications usually refers to traditional telecommunications networks. These networks can include cable infrastructures, whether wire or optical cable, as well as inter-connections with wireless networks, including mobile telephone systems and microwave transmission systems.

Today, mobile communications are facilitated also by a system of special wireless or satellite networks. Computer networks may also consist of an independent fixed cable infrastructure, but are more frequently operated as a virtual network by connections made through telecommunication infrastructures, thus permitting the creation of computer networks or linkages of networks that are global in nature.

The communications in respect of which the traffic data may be collected or recorded, however, must be specified. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

The article should not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems.

However, if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to take the necessary measures to engage such capability.

Real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Interception is surreptitious and must be carried out in such a manner that the communicating parties will not perceive the operation. Service providers and their employees knowing about the interception must, therefore, be under an obligation of secrecy in order for the procedure to be undertaken effectively.

Provision could compel a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data.

Safeguards or conditions should exist to impose reasonable time periods for the duration of the obligation, given the surreptitious nature of the investigative measure.

3.6 About Interception of content data (Article 21)

Given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography).

'Content data' refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication. It is everything transmitted as part of the communication that is not traffic data.

Most of the elements of this article are identical to the real-time collection of computer data. Therefore, the comments, above, concerning the collection or recording of traffic data, obligations to co-operate and assist, and obligations of confidentiality apply equally to the interception of content data.

Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences'.

Also, as set forth in the comments above on Article 20, the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data.

Therefore, the real-time interception of content data of computer communications is just as, if not more, important as is the real-time interception of telecommunications.

3.7 Special circumstances that should be taken into account while exercising procedural powers

Besides these, we should consider some other circumstances on which the court, both in first instance and in the second instance proceedings must bear in mind throughout the criminal proceedings.

In addition to the unquestionable determining when, how and where the criminal offence was committed, it is sometimes necessary to determine the level of technical knowledge which was needed for the successful execution of the criminal act, because if the actions taken were more refined the number of potential perpetrators is fewer.

Furthermore, it is necessary for certain forms of criminal offences where the offender is an official to establish the required level and availability of passwords, codes, crypto keys, data organization, etc., which were essential for the execution of the crime, and which can often indicate whether the crime was committed by an employee or someone from the outside. Then attention must be paid to the list of employees who according to their job description have the ability to be the perpetrators of the criminal offence. Sometimes it is important to determine possible motives for committing the crime, it is important to examine witnesses according to their knowledge of the important facts and then, as always, to assess their credibility, reliability etc. In this kind of cases it is sometimes important to identify the existing weaknesses in the protection system and to whom they were known, and who are the persons who can be fully informed regarding the commission of the offense.

In order to achieve a better understanding of these problems in a situation when the court must apply the law in an area which is still insufficiently known, an expert witness must provide all relevant information on the seized computer, network configuration, peripheral devices, operating system, software for managing databases, program languages, data carriers and organization of data on them, the programs used for examination and the like. Judges and prosecutors must be prepared to ask all the necessary questions without hesitation answers to which will clarify all doubts.

It is very important that there is special caution when assessing the data provided on data carriers such as listings, magnetic tapes, disks, etc. Firstly, it is very important to determine that what is obtained is what was actually required, and that it suits the requirements of "authenticity" and the best evidence. Proving authenticity involves submitting acceptable proof that the presented document was actually generated from a precisely defined computer at a precise time by a particular program.

Using computers as a means to commit various criminal offences from the Criminal Code is increasing (unauthorized production, possession and circulation of narcotic drugs; child abuse, human trafficking; mediation in prostitution; for use of system for electronic transfer of money; money laundering; extortion; blackmail; forgery of money; advertising and sales of harmful products on the Internet; terrorism etc.)

Increase in the number of juvenile perpetrators of these crimes is also significant, because an increasing number of young people who during their education in primary and secondary schools acquire basic computer knowledge represent a huge potential for all kinds of misuse of computers.

The court is authorized to freely evaluate expertise of evidence on the basis of conscientious and careful assessment of all the circumstances. The court is obliged to submit expert opinion to logical analysis, and is not bound by the expert's findings and opinion. Even though the court has no expert knowledge there is a possibility that an expert opinion is not accepted when the court finds that the views could not resist the criticism based on the rules of logical reasoning and experience. If the court doubts the results of expertise, it is authorized to undertake whatever is necessary to remove such doubts or to order a new expertise.

In some more complex cases it is difficult to exert effective control over the work of an expert. In these proceedings, the first instance court is not bound to use the official list of experts, in the sense that it would be a restriction of its freedom in the choice, especially for cases involving cyber crime which have been increasing daily, and bearing in mind there are not enough experts for the amount of material that require expertise. An expert has to give his opinion and to explain it, and there is of course the right to directly ask him questions. This right applies to the parties in the proceedings and to judges, including the members of the panel.

If any party raised specific objections to the findings and opinion of an expert, it is not enough that they are answered in general terms. On the other hand, the parties cannot claim without proof that the opinion of an expert is unprofessional or his findings incomplete or that the expert is biased. It should be borne in mind that the expert shall be summoned to comment directly but only if the parties put specific, quality objections, and not when it leads only to the prolongation of the proceedings. In assessing the findings and opinions the court should take into consideration whether what was demanded from an expert was completely clear, whether the request were specific and precise.

4. Mutual Legal Assistance

4.1 About General principles

It should be clear that international co-operation is to be provided "to the widest extent possible." This principle requires jurisdictions to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally.

Co-operation is to be extended to all criminal offences related to computer systems and data, as well as to the collection of evidence in electronic form of a criminal offence.

Co-operation is to be carried out both in accordance with the provisions of the Convention and through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws".

The latter establishes the general principle that the provisions of Convention do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto, or relevant provisions of domestic law pertaining to international co-operation.

4.2 About General principles relating to mutual assistance

If legal framework is based on Convention, it will clarify that the obligation to provide mutual assistance is generally to be carried out pursuant to the terms of applicable mutual legal assistance treaties, laws and arrangements.

It will be also required to have a legal basis to carry out the specific forms of co-operation described in the remainder of the Chapter, if its treaties, laws and arrangements do not already contain such provisions.

Some Parties will not require any implementing legislation in order to apply the provisions referred to, since provisions of international treaties that establish detailed mutual assistance regimes are considered to be self-executing in nature. It is expected that authority will either be able to treat these provisions as self-executing, already have sufficient flexibility under existing mutual assistance legislation to carry out the mutual assistance measures established under this Chapter, or will be able to rapidly enact any legislation required to do so.

Also, to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to, should be noted.

Provisions should be in place for empowering the competent authority to make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems; and requiring the requested authority to use expedited means to respond to requests in such circumstances.

Provisions should set forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. These regimes provide safeguards for the rights of persons located in the requested Party that may become the subject of a request for mutual assistance.

Dual criminality for purposes of mutual assistance is a standard.

4.3 About Specific provision for Mutual assistance and International cooperation

Specific provisions will be analyzed in the separate document.

5. Specific Guidelines

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved". This is to ensure that new forms of malware or crime would always be covered by the Convention.

5.1 About notion of "computer system" (Guidance Note #1)

Article 1.a of the Convention defines "computer system" as any "device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data". The T-CY agrees that this definition includes, for example, modern mobile telephones which are multifunctional and have among their functions the capacity to produce, process and transmit data, such as accessing the Internet, sending e-mail, transmitting attachments, upload contents or downloading documents.

Similarly the T-CY recognises that personal digital assistants, with or without wireless functionality, also produce, process and transmit data.

T-CY agrees that the definition of "computer system" in Article 1.a covers developing forms of technology that go beyond traditional mainframe or desktop computer systems, such as modern mobile phones, smart phones, PDAs, tablets or similar.

5.2 About botnets (Guidance Note #2)

The term 'botnet' may be understood to indicate:
"a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'".

Relevant articles of the Convention and national law should be the one providing criminal law provisions on Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, Computer related forgery, Computer related fraud and Infringements related to copyrights and related rights.

5.3 About Transborder access to data (Guidance Note #3)

With regard to Article 32a (transborder access to publicly available (open source) stored computer data) no specific issues have been raised and no further guidance by the T-CY is required at this point.

It is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public.

If a portion of a public website, service or similar is closed to the public, then it is not considered publicly available in the meaning of Article 32a.

Regarding Article 32b, typical situations may include:
☐ A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.16
☐ A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.

Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.

As pointed out above, it is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.

On the notion of "transborder" and "location"
Transborder access means to "unilaterally access computer data stored in another Party without seeking mutual assistance".20

On the notion of "access without the authorisation of another Party"

Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

On the notion of "consent"

Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived.

On the applicable law

In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

On the person who can provide access or disclose data

As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances, laws and regulations applicable.

On the location of the person consenting to provide access or disclose data

The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party.

However, multiple situations are possible. It is conceivable that the physical or legal person is located in the territory of the requesting law enforcement authority when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access.

5.4 About identity theft and phishing in relation to fraud (Guidance Note #4)

While there is no generally accepted definition or consistent use of the term, identity theft commonly involves criminal acts of fraudulently (without his or her knowledge or consent) obtaining and using another person's identity information. The term "identity fraud" is sometimes used as a synonym, although it also encompasses the use of a false, not necessarily real, identity.

Related acts may include "phishing", "pharming", "spear phishing", "spoofing" or similar conduct, for example, to obtain password or other access credentials, often through email or fake websites.

The T-CY agrees that the following illustrates the various scope and elements of identity theft and phishing and the criminal provisions that may apply: Illegal access, Illegal interception, Data

interference, System interference, Computer related forgery, Misuse of devices and Computer related fraud.

5.5 About DDOS attacks (Guidance Note #5)

Denials of service (DOS) attacks are attempts to render a computer system unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users.

Distributed denials of service (DDOS) attacks are denial of service attacks executed by many computers at the same time.

There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users and sending more e-mails to e-mail servers than the system can receive and handle.

The T-CY agrees that the following illustrates the various scope and elements of criminal law provisions and multi-functional criminal use of such attacks: Illegal access, Data Interference and System interference.

5.6 About Critical information infrastructure attacks (Guidance Note #6)

Critical infrastructures can be defined as systems and assets, whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety, or any combination of those matters. Countries define critical infrastructures differently. However, many countries consider critical infrastructures to include the energy, food, water, fuel, transport, communications, finance, industry, defence and governmental and public services sectors.

T-CY agrees that following list of Articles related to critical information infrastructure attacks illustrates their multifunctional criminal use: Illegal access, Illegal interception, Data interference, System interference, Computer related forgery and Computer related fraud.

5.7 About New forms of malware (Guidance Note #7)

There are many current forms of malware, which has been defined by the Organization for Economic

Cooperation and Development as "a general term for a piece of software inserted into information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners." Commonly-known forms include worms, viruses, and trojans.

Current forms of malware can steal data by copying it and sending it to another address; they can manipulate data; they can hinder the operation of computer systems, including those that control critical infrastructures; ransomware can delete, suppress or block access to data; and specially-tailored malware can target specified computer systems.

T-CY agrees that following list of Articles related to critical information infrastructure attacks illustrates their multifunctional criminal use: Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, Computer related forgery and Computer related fraud.

5.8 About Spam (Guidance Note #8)

Spam is often defined as unsolicited bulk email, where a message is sent to a significant number of email addresses, where the recipient's personal identity is irrelevant because the message is equally targeted at many other recipients without distinction.

There are separate issues relating to:
☐ the content of spam,
☐ the action of sending spam, and
☐ the mechanism used to transmit spam.

The content of spam may or may not be illegal, and where the content is illegal (such as offering fake medicines or fraudulent financial offerings) the offence may fall under the relevant national legislation for those offences. The action of transmitting spam (including bulk transmission of non-objectionable content) may be a civil or criminal offence in jurisdictions.

T-CY agrees that following list of Articles related to critical information infrastructure attacks illustrates their multifunctional criminal use: Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, Computer related fraud and Offences related to infringements of copyright.

5.9 About Production orders for subscriber information (Guidance Note #10)

Article 18.1.b is restricted to circumstances in which the criminal justice authority issuing the production order has jurisdiction over the offence.

This may include situations in which the subscriber is or was resident or present in that territory when the crime was committed. The present interpretation of Article 18 is without prejudice to broader or additional powers under the domestic law of Parties.

Agreement to this does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State nor creates new obligations or relationships between the Parties.

What are the characteristics of a "production order?"

A "production order" under Article 18 is a domestic measure and is to be provided for under domestic criminal law. A "production order" is constrained by the adjudicative and enforcement jurisdiction of the Party in which the order is granted.

Production orders under Article 18 refer: to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

What effect does the location of the data have?

The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the service provider.

The Explanatory Report states with respect to:

☐ Article 18.1.a that "the term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory."

☐ Article 18.1.b that "the term 'possession or control' refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company)."

Regarding Article 18.1.b, a situation may include a service provider that has its headquarters in one jurisdiction, but stores the data in another jurisdiction. Data may also be mirrored in several jurisdictions or move between jurisdictions according to service provider discretion and without the knowledge or control of the subscriber. Legal regimes increasingly recognise that, both in the criminal justice sphere and in the privacy and data protection sphere, the location of the data is not the determining factor for establishing jurisdiction.

With regard to Article 18.1.b, Parties could consider that a service provider is "offering its services in the territory of the Party", when:

☐ the service provider enables persons in the territory of the Party to subscribe to its services51 (and does not, for example, block access to such services);

and

☐ the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

The production of subscriber information under Article 18 Budapest Convention could, therefore, be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers:

if the criminal justice authority has jurisdiction over the offence and if the service provider is in possession or control of the subscriber information, and if the person (service provider) is in the territory of the Party or a Party considers that a service provider is "offering its services in the territory of the Party" when, for example the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services), and the service provider has established a real and substantial connection to a Party (relevant factors include the extent to which a service provider orients its activities toward such subscribers for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party, and if the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party.

5.10 About Terrorism (Guidance Note #11)

Many countries are Parties to numerous treaties, and subject to UN Security Council Resolutions, that require criminalization of different forms of terrorism, facilitation of terrorism, support for terrorism, and preparatory acts. In terrorism cases, countries often rely on offenses that derive from those topics specific treaties, as well as additional offenses in national legislation.

The Budapest Convention is not a treaty that is focused specifically on terrorism. However, the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

The T-CY agrees that the substantive crimes in the Convention may also be acts of terrorism as defined in applicable law.

The substantive crimes in the Convention may be carried out to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

The procedural and mutual legal assistance tools in the Convention may be used to investigate terrorism, its facilitation, and support for it, or preparatory acts.

6. Glossary of terms

Glossary terms and definitions are cited from Electronic Evidence Guide of the Council of Europe. However, some were collected from the open sources such web sites as well. Credit belongs to the original authors, especially to Peter Day and Denis Howe, from whose glossary most of those terms were collected.

1-10

3G networks: 3G or **3rd generation mobile telecommunications** is a generation of standards for mobile phones and mobile telecommunication services fulfilling the **International Mobile Telecommunications-2000 (IMT-2000)** specifications by the International Telecommunication Union. Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment.

4G is the fourth generation of broadband cellular network technology, succeeding 3G. A 4G system must provide capabilities defined by ITU in IMT Advanced. Potential and current applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, and 3D television. The first-release Long Term Evolution (LTE) standard (a 4G candidate system) has been commercially deployed in Oslo, Norway, and Stockholm, Sweden since 2009. It has, however, been debated whether first-release versions should be considered 4G, as discussed in the technical understanding section below.

A

Access: The reading or writing of data; as a verb, to gain entry to data. Most commonly used in connection with information access, via a user ID, and qualified by an indication as to the kinds of access that is permitted. For example, read-only access means that the contents of the file may be read but not altered or erased.

Access Control Lists (ACLs): is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.

Access token: is an object encapsulating the security descriptor of a process. Attached to a process, a security descriptor identifies the owner of the object (in this case, the process) and ACLs that specify access rights allowed or denied to the owner of the object. While a token is used to represent only the security information, it is technically free-form and can enclose any data. The access token is used by Windows when the process or thread tries to interact with objects whose security descriptors enforce access control (*securable objects*).

Access time: the time interval between the instant that data is requested and the instant that it is received.

Account: subscription to a networked computer system.

Account name: same as login ID or user ID. The word you type at the "Login:" prompt; your electronic name.

Address: A character or group of characters that identify a register, a location or some other data source or destination.

Aggregate: total created from smaller units. For instance, the population of a county is an aggregate of the populations of the cities, rural areas, etc. that comprise the county.

Aggregate data: data that have been aggregated.

Algorithm: A set of rules for solving a problem in a given number of steps.

Alias: see nickname.

Analog: a method of storing information, used by most audiotapes, videotapes and laserdiscs (and all LP phonograph records, remember those?). An analog device uses a physical quantity, such as length

or voltage, to represent the value of a number. By contrast, digital storage relies on a coding system of numeric units.

Application Layer: layer seven of the OSI reference model. It serves as a means by which applications access communications services.

Application: the use to which a data processing system is put within a given discipline, such as a payroll application, an airline reservation application or a network application.

Application program: a program that is written for or by a user that applies to the user's discipline.

Application software: a group of programs designed to perform tasks that can be tailored to a user's specific needs.

Archive: to copy programs and data onto an auxiliary storage medium (disk, tape, etc.) for long-term retention, such as when disk space has become full.

A file with a structure that allows storage of multiple files within it in such a way that the names of the files can be listed and files can be individually added and deleted. The terminology is typically associated with microcomputers. On a mainframe, such a file is typically called a library.

Argument: a value supplied to a procedure, macro, subroutine, or command that is required in order to evaluate that procedure, macro, subroutine, or command. Synonymous with parameter.

ASCII: American Standard Code for Information Interchange (pronounced ask-ee). The form in which text characters are handled in most computer systems and networks. ASCII text has no special characters for formatting such as underlined or bold characters, font changes, etc., thus can be viewed on any personal computer or terminal.

Assembler: a program that converts symbolically-coded programs into object level, machine code. In an assembler program, unlike a compiler, there is a one-to-one correspondence between human-readable instructions and the machine-language code.

Authentication: process of establishing who you are.

Authorization: permission to access non-public information or use equipment that is either fully or partially restricted.

Autonomous system: a collection of one or more networks that are administrated by the same entity. Each regional network (such as SURAnet) is an autonomous system.

Acquisition: a process referred to as Imaging. The duplicate is created using a hard-drive duplicator or software imaging tools such as DCFLdd, IXimager, Guymager, TrueBack, EnCase, FTK Imager or

FDAS. The original drive is then returned to secure storage to prevent tampering. The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state. In corporate environments seeking civil or internal charges, such steps are generally overlooked due to the time required to perform them.

Active data: Files and folders that reside in the IT system storage units that are accessible and visible to the users in an immediate and direct manner by the means of the operating system's tools.

AfriNIC (**African Network Information Center**): is the regional Internet registry (RIR) for Africa.

Amazon S3 (**Simple Storage Service**): is an online storage web service offered by Amazon Web Services. Amazon S3 provides storage through web services interfaces (REST, SOAP, and BitTorrent). Amazon launched S3, its first publicly-available web service, in the United States in March 2006 and in Europe in November 2007.

API: An **application programming interface** is a specification intended to be used as an interface by software components to communicate with each other. An API may include specifications for routines, data structures, object classes, and variables. An API specification can take many forms, including an International Standard such as POSIX or vendor documentation such as the Microsoft Windows API, or the libraries of a programming language, e.g. Standard Template Library in C++ or Java API.

APNIC (Asia Pacific Network Information Centre): is the regional Internet registry for the Asia Pacific region. APNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations.

ARIN (American Registry for Internet Numbers): is the Regional Internet Registry (RIR) for Canada, many Caribbean and North Atlantic islands, and the United States. ARIN manages the distribution of Internet number resources, including IPv4 and IPv6 address space and AS numbers.

Assistant (PDA): They come in many forms and sizes and usually have storage capability built in in the form of hard disks or flash memory. They have become very popular in recent years and may be useful sources of electronic evidence as they run their own operation systems and are often connected to the internet via **WLAN**, **3G** or **LTE** networks.

ATM: An automatic teller machine (ATM), is a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller (from Wikipedia)

Autonomous System: is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet.

Azure: Microsoft Windows Azure Platform is a Microsoft cloud computing platform used to build, host and scale web applications through Microsoft data centers. Azure is classified as platform as a service and forms part of Microsoft's cloud computing strategy, along with its software as a service offering, Microsoft Online Services. The platform consists of various on-demand services hosted in Microsoft data centers and commoditized through three product brands. These are Windows Azure (an operating system providing scalable compute and storage facilities), SQL Azure (a cloud-based, scale-out version of SQL Server) and Windows Azure AppFabric (a collection of services supporting applications both in the cloud and on premise). Microsoft has announced free Ingress for all the customers of Azure from 1 July 2011.

B

Backup: A copy taken of all information held on a computer in case something goes wrong with the original copy.

Biometric scanners: a device connected to a computer system that recognizes physical characteristics of an individual (e.g., fingerprint, voice, retina).

BIOS: Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

Bit: A **bit** (a contraction of **binary digit**) is the basic capacity of information in computing and telecommunications; a bit represents either 1 or 0 (one or zero) only. The representation may be implemented, in a variety of systems, by means of a two state device. In computing, a bit can also be defined as a variable or computed quantity that can have only two possible values. These two values are often interpreted as binary digits and are usually denoted by the numerical digits 0 and 1. The two values can also be interpreted as logical values (*true*/*false*, *yes*/*no*), algebraic signs (+/−), activation states (*on*/*off*), or any other two-valued attribute. The correspondence between these values and the physical states of the underlying storage or device is a matter of convention, and different assignments may be used even within the same device or program. The length of a binary number may be referred to as its "bit-length."

Bluetooth: A telecommunications industry specification that describes how mobile phones, computers, and PDAs can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection. Bluetooth requires that a low-cost transceiver chip be included in each device.

Blu-ray Disc (BD): is an optical disc storage medium designed to supersede the DVD format. The plastic disc is 120 mm in diameter and 1.2 mm thick, the same size as DVDs and CDs. Blu-ray Discs contain 25 GB per layer, with dual layer discs (50 GB) being the norm for feature-length video discs. Triple layer discs (100 GB) and quadruple layers (128 GB) are available for *BD-XL* re-writer drives.

Backbone: refers to a piece of cable used to connect different floors or departments together into a network. Also generalized to a network that connects networks together.

Background processing: users may use a terminal for one project and concurrently submit a job that is placed in a background queue that the computer will run as resources become available. Also refers to any processing in which a job runs without being connected to a terminal.

Backspace: a keyboard operation that moves the cursor one place to the left. A destructive backspace erases characters as it goes, thus allowing users to modify what has been typed (distinguished from the left- arrow key).

Backup: a resource that is or can be used as a substitute when a primary resource fails or when a file has been corrupted. To save as in to make a copy in case of future failure or corruption.

Bandwidth: a piece of the spectrum occupied by some form of signal, where it is television, voice, fax data, etc.. Signals require a certain size and location of bandwidth in order to be transmitted. The higher the bandwidth, the faster the signal transmission, and thus allowing for a more complex signal such as audio or video. Because bandwidth is a limited space, when one user is occupying it, others must wait their turn. Bombarding the Internet with unnecessary information is referred to as "taking up bandwidth".

BASIC: Beginners All-purpose Symbolic Instruction Code. A commonly used personal-computer language, first developed at Dartmouth during the 1960s.

Batch processing: originally, a method of organizing work for a computer system, designed to reduce overhead by grouping similar jobs. In one scheme, jobs were collected into batches, each requiring a particular compiler. The compiler was loaded, and the jobs submitted in sequence to the compiler. The term has come to be applied to background processing of jobs not requiring user intervention on multiuser systems. See compiler.

Binary: a file containing one or more strings of data bits which are not printable characters. Some binary files may be computer programs or other forms of data that contain no text characters at all. Binary files cannot be displayed on screen, but can be downloaded for use with appropriate applications on your computer. Binary (base 2) is also the building block of computer information, representing "on" or "off" and "true" or "not true" as 1 or 0.

Binary number: a number written using binary notation which only uses zeros and ones. Example: decimal number seven in binary notation is: 111.

Bit: a binary digit, either a 0 or 1. In the U. S., 8 bits make up one byte; in Europe, byte equals one word.

Bits per second (bps): the speed at which bits are transmitted.

Block: a sequence of words or characters written contiguously, such as into a group, by a computer and stored on a disk, diskette, magnetic tape, etc.

Bold: a way of emphasizing a word of text, as in darker type or brighter characters on a video display terminal.

Booting: turning on computer.

Break: an interruption to a transmission; usually a provision to allow a controlled terminal to interrupt the controlling computer.

Bridge: a device that connects two networks and passes traffic between them based only on the node address, so that traffic between nodes on one network does not appear on the other network. For example, an Ethernet bridge only looks at the Ethernet address.

Broadband: a communications medium on which multiple signals are simultaneously transmitted at different frequencies. Also refers to switching capability implemented on this medium that allows communication between devices connected to it. In telecommunications it is defined as any channel with a bandwidth greater than voice grade (4 KHz).

Broadcast: a single message addressed to all nodes on a network.

Browser: a software tool used to read electronic documents. Mosaic, NetScape and Lynx are the most popular browsers.

Buffer: a temporary memory for data, normally used to accommodate the difference in the rate at which two devices can handle data during a transfer.

Bug: an error. Can be a hardware malfunction or a software programming error.

BUS topology: network wiring commonly used by Ethernet in which all nodes on the network see all packets.

Byte: a group of adjacent binary digits, usually 8, on which a computer operates as a unit; often used to represent a single character (see bit).

C

Capturing data: Capturing data means to copy data from a computer system or electronic media and store them on an external storage media before verifying the integrity of the data where possible (e.g. not possible for capturing RAM). Capturing data can also be possible for network data. In this context on machine in the network is used to capture the network packets and store their information to a file (e.g. in PCAP format).

CentralOps: CentralOps is a website offering investigative lookup opportunities like a domain dossier, email dossier, whois lookups, etc. These services can provide information about IP-addresses, domains and email addresses. The website is run by Hexillion is a privately-held company based in the USA. Its' address is: http://centralops.net

Chat logs: is an archive of transcripts from online chat and instant messaging conversations. Many chat or IM applications allow for the client-side archiving of online chat conversations, while a subset of chat or IM clients (i.e., Google Talk and Yahoo! Messenger 11 Beta) allow for the saving of chat archives on a server for future retrieval. The latter trend has been adopted by the applications' vendors because of the decreasing cost of web server hard drive space.

CIDR notation: is a compact specification of an Internet Protocol address and its associated routing prefix. Classless Inter-Domain Routing (CIDR) is an Internet Protocol (IP) address allocation and route aggregation methodology[1] used within the Internet addressing architecture that replaced the IPv4 classful network organization of the IP address space. It is used also for IPv6 networking, the next generation of the IP addressing architecture.

Circuit boards: A thin plate with chips, devices and other electronic components installed on the plate (also referred to as the printed circuit board).

Closed Circuit Television (CCTV): They are used by companies, governments and individuals for security and may provide evidence that certain activities have or have not taken place.

Cloud: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[…]

CMOS: Complementary metal-oxide semiconductor. Semiconductor technology used in the transistors that are manufactured into most of today's computer microchips. It commonly holds the BIOS preferences of the computer through power off with the aid of a battery (adapted from).

COFEE: Computer Online Forensic Evidence Extractor is a tool kit, developed by Microsoft, to help computer forensic investigators extract evidence from a Windows computer. Installed on a USB flash drive or other external disk drive, it acts as an automated forensic tool during a live analysis. Microsoft provides COFEE devices and online technical support free to law enforcement agencies.

Compact Disk (CD): Optical disc 12cm in diameter used for storing binary information. Its formatted capacity is between 640-700 Mb and was primarily used to store audio. When used for storing generic data it is called CD-ROM.

Computer Memory: Memory is the electronic holding place for instructions and data that a computer's microprocessor can reach quickly. RAM is located on one or more microchips installed in a computer.

Computer Networks: consists of connections between two or more computers that are linked by data cables or by wireless connectivity. These computers are able to share data and other resources between them. They often have other hardware components to enable the scope of activities required of the network.

Cookie: Cookies are small files that the internet server downloads onto the hard drive of the user's computer. These files contain specific information that identifies the user (for example, through passwords and lists of websites visited).

CPU: Central processing unit. The computational and control unit of a computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic, and control functions in a computer.

Cracker: A Cracker is a person that enters into a system without authorisation with the intention of causing some form of damage or to make beneficial gain.

Cybercrime: refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cybersquatter: A Cybersquatter is a person that reserves or buys domain names with the intention of selling them to interested companies in the future.

Cell relay: packet-switching using small, fixed-sized packets called cells. The fixed size allows for very high speed switching. It is the basis for SMDS and ATM.

Channel: any medium by which information can be transmitted. For example, the air is a channel for our voices just as much as a fiber optic line can be data for a video signal.

Character: any symbol (usually alphabetic, numeric, or punctuation) that can be entered into your computer.

Character set: a set of characters handled by a specified machine; sets include alphabetic characters, numbers, symbols, graphics characters, a space character and control characters. Graphics characters denote a printed mark; control characters produce some particular effect. Two of the most widely used sets are ASCII and EBCDIC.

Chip: a tiny piece of semi-conductive material, usually based on silicon, used in the manufacture of electronic components.

Client: a computer program that uses the services of another computer program. Software that extracts information from a server; your auto-dial phone is a client, and the phone company is its server.

Client/server: a relationship in which client software obtains services from a server on behalf of a person.

Client-Server Interface: an architecture that provides for the splitting of user requests (usually called clients) and a related server function, most commonly across a network. The combined effect is to provide the clients with access to some service such as databases, printing, etc.

Code: a language for expressing operations to be performed by a computer.

Command: a request, typed from a terminal or embedded in a file, to perform an operation or to execute a particular program.

Communications line: a physical medium (wire, microwave beam) used to transmit data.

Communications program: a program that makes a computer act as a terminal to another computer. Communications programs usually provide for file transfer between microcomputers and mainframes.

Compiler: a program that translates human-readable programs into a form the computer understands. The input (source code) to the compiler is a description of an algorithm in a problem-oriented language; its output (object code) is an equivalent description of the algorithm in a machine-oriented language.

Computer: a device or system that is capable of carrying out a sequence of operations in a distinctly and explicitly defined manner. The operations are frequently numeric computations or data manipulations, but also include data input and output. The ability to branch within sequences is its key feature.

Conference: an electronic meeting place dedicated to a particular subject where users come to participate in discussions or group projects. Conferences can be used to post a variety of information such as news services, newsletters, and statistics; also called "newsgroups," "bulletin boards," or

"echoes." An electronic conference provides a many-to-many communication medium, as opposed to the person-to-person nature of e-mail. All conferences have a particular subject or purpose, and the topics and responses they contain might provide items of news, ideas, questions, or other information in almost any form. Some special-purpose conferences may have restricted access, allowing some users to write messages, some only to read, and some neither. The person responsible for the technical maintenance and/or community communication is called the "conference facilitator."

Configuration: the particular hardware elements and their interaction in a computer system for a particular period of operation.

Connect time: time that elapses while the user of a terminal is connected to a time-sharing system; it is measured by the duration between logon and logoff.

Control character: one of 32 characters of the ASCII character set that defines a control function for a character entry and display device such as a terminal. Examples are carriage return, tab, form feed and bell.

Control key: a special function key on a computer keyboard, frequently used in combination with alphabetic keys, to enter commands.

Copy: a function that reads data from a source, leaving the source data unchanged and writes it elsewhere. One example would be to copy a deck of punched cards onto magnetic tape.

Crash: a computer system is said to crash when it stops working for some reason and must be restarted.

Cursor: a symbol on a display screen that indicates the position at which the next character entered will be displayed. The symbol often blinks so that it can be easily noticed.

Cursor control: the keyboard keys used to position the cursor on a display screen. They are usually keys labeled with arrows indicating the direction of movement.

Cyberspace: the nebulous "place" where humans interact over computer networks (the Internet is considered Cyberspace). Coined by William Gibson in Neuromancer.

D

DAT (Digital Audio Tape): Digital audio tape used for storing media on *back-up* systems.

Data storage devices: A **data storage device** is a device for recording (storing) information (data). Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs.

DATABASE: Structured collection of data that can be accessed in many ways. Common database programs are: Dbase, Paradox, Access. Uses: various including – address links, invoicing information, etc.

Dead box forensics: Dead box forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Dead box forensics follow this aim but is only focused on storage media in computer systems that are in a turned off state.

Deleted data: Files and folders that existed previously on the computer as active data but since have been deleted by the operating system or the end-user. Deleted data will remain in the storage unit until they are overwritten by another file.

Desktops: The term has been adopted as an adjective to distinguish office appliances (such as photocopiers and printers) which can be fitted on top of a desk, from larger equipment covering its own area on the floor. Desktop may also refer to Desktop computer, a personal computer designed to fit on a desk

Digital Forensics: Digital Forensics is a branch of forensic science related to the acquisition, processing, analysis and reporting of evidence that is stored on computer systems, digital devices and other storage media with the aim of admissibility in court.

Digital media: is a form of electronic media where data are stored in digital (as opposed to analogue) form. It can refer to the technical aspect of storage and transmission (e.g. hard disk drives or computer networking) of information or to the "end product", such as digital video, augmented reality or digital art.

Digital photography: Digital photography is a form of photography that uses an array of light sensitive sensors to capture the image focused by the lens, (from Wikipedia)

Digital Video Disk (DVD): Digital Versatile (video) Disc. Presently the natural successor of the CD for the reproduction of quality sound and image.

DIGITAL VIDEO: Video captured, manipulated and stored in a digital format.

Digitalisation: To store electronic information as a chain of "ones" and "zeros". Due to the fact that as many "zeros" as "ones" can be easily represented by 2 voltaic levels in electronic media, the binary numbering system is widely used in the digital IT world.

Diskette Proprietary tools: IT applications that have been developed expressly in keeping with the functionalities and the operation of the company that utilises it and that, in general, are not available for purchase on the open market.

Diskette: Form of media storage, becoming less frequently used, that consists of a circular piece of magnetic material within a plastic case / covering.

DNS: Domain Name System (DNS). Transforms the name of a domain, for example www.cybex.es, into the IP address where the server that you are looking for is situated.

Docking stations: A device to which a portable computer (e.g., laptop, notebook) can be attached for use as a desktop computer, usually having a connector for externally connected devices such as hard drives, scanners, keyboards, monitors, and printers.

Domain name: The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A **Domain Name Service** resolves queries for domain names (which are easier to understand and utilize when accessing the internet) into IP addresses for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com translates to the addresses `192.0.43.10` (IPv4) and `2620:0:2d0:200::10` (IPv6).

DomainTools: DomainTools, LLC provides a directory of domain name Whois ownership records that serves as a comprehensive snapshot of past and present domain name registration and ownership records that span more than a decade of Internet history. In addition to Whois data, DomainTools offers a set of research tools that helps individuals and organizations discover and monitor everything about a domain name. DomainTools is also known for offering advanced semantic name suggestion technology, patented Reverse IP technology, and incorporating millions of screenshots into a combined screenshot history view of how a website looks now and how it used to look like in the past.

Dongle: is a small piece of hardware that plugs into an electrical connector on a computer and serves as an electronic "key" for a piece of software; the program will run only when the dongle is plugged in. The term "dongle" was originally used to refer only to software-protection dongles; however, currently "dongle" is often used to refer to any small piece of hardware that plugs into a computer. This article is limited in scope to dongles used for the purpose of copy protection or authentication of software to be used on that system.

Drive duplicators: A device for fast copying (duplicating) of different storage media, e.g., hard disks or CDs.

DropBox: is a file hosting service operated by Dropbox, Inc. that offers cloud storage, file synchronization, and client software.

Dynamic Host Configuration Protocol (DHCP): is a protocol used to automatically assign a pool of IP addresses to a group of devices.

Data: information suitable for communication, interpretation or processing by a computer.

Data communications: the collection and redistribution of data through communications channels, often including operations such as coding, decoding and validation.

Data entry: the entry of data into a computer or onto a computer-readable medium by an operator from a single data device, such as a card reader or keyboard.

Data processing: the systematic performance of operations upon data, for example, handling, merging, sorting and computing.

Dataset: a file or group of files associated with one part of a study.

Database management system: a systematic approach to storing, updating, securing and retrieving information stored as data items, usually in the form of records in one or more files.

DBMS: Data Base Management System.

Debug: to detect, trace and eliminate errors in computer programs.

Default: a software function or operation which occurs automatically unless the user specifies something else.

Dial-up: to connect to a computer by calling it on the telephone.

Digital: used in computers to describe information that can be represented by a collection of bits.

Direct access: the ability to read or write data directly from or to any location on a storage device without having to refer to data that was previously written. Files written with direct access do not have to be read sequentially starting at the beginning.

Directory: a logical container of files and other directories; synonymous with folder. Typically implemented as a file that contains pointers (directions) to files or other directories.

Distributed: processing resides in more than one computer in a network.

Distributed application: application designed so that components run on different - but cooperating - systems on a network.

Distributed database: the data resides in more than one physical database in a network. Access to the data involves more than one database server. Clients may have to connect to more than one server directly and integrate the data they receive according to the applications needs.

Distributed file system: allows files on remote nodes of a network to appear locally connected.

DOS: Disk Operating System. A Microsoft program that controls a computers transfer of data to and from a hard or floppy disk. DOS generally refers to the operating systems for the IBM PCs and their clones. Also the name of an old operating system on IBM mainframes.

Dot-matrix printer: a printer that creates each character from an array of dots. The dots are formed by pins striking a ribbon against the paper, one pin for each dot position. The printer may be a serial printer (printing one character at a time) or a line printer.

Down: a computer is down when it is not running. It may be shut down for maintenance, hardware failure, or failure of the operating system or user program.

Download: the transfer of information from a remote computer system to the users system. Opposite of upload.

Downtime: the time interval during which equipment is nonfunctional.

Drag and drop: a protocol supported by OPEN LOOK and Macintosh System 7 that allows a user to specify the input file to an application by dragging the icon representing the file onto the applications icon and dropping it there. OPEN LOOK also recognizes dragging the icon into the applications input panel. For example, dragging a files icon into the printool application causes it to be printed.

Drive: a generic term used to identify the equipment that serves as a player or recorder for a storage medium.

Dump: a printed representation of the contents of a computer storage device, usually main memory, backed-up when a system crash or other failure has occurred. As a verb, refers to a large amount of data.

E

Electronic evidence: Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well defined processes using specialised personnel and operating within an adequate legal framework.

E-mail virus: Viruses cannot travel in e-mail messages because they only use a 7 bit format to transfer text. The only way that they can travel is by binary files that are sent as attachments with the text message. It is recommended to check these files with an anti-virus before opening.

Email: The exchange of computer-stored messages by telecommunication

E-mail address: the way you specify where an E-Mail message should be delivered.

E-mail server: a computer system that provides MTA, mailbox storage and directory services and optionally UA services.

E-mail service: UA, MTA, mailbox storage, and directory service.

Encryption: Method of scrambling and encoding data. Used to convert plain text into ciphertext (by using a mathematical parameter called cryptographic key) in order to prevent anyone but the intended recipient from reading that data.

Environment: the setting in which computing takes place that is the aggregate of the hardware, software, policies and procedures relating to their use. The computing environment may be influenced by software, such as the operating system (for example, a UNIX environment) or the vendor (for example, an IBM environment).

Environmental data: Refers, as a whole, to the data that is not active on the IT system. Environmental data includes: Data found in unused or unassigned areas, Data found in the "Slack" file space and File data that has been deleted that is not visible using the operating system tools.

Ethernet: a local area network originally developed by Xerox for linking personal computers. Later adapted by DEC and Intel as well and subsequently adopted as an international standard called 802.3. It transmits data at 10 megabits per second. All computers on a network were originally connected to a coaxial cable up to one kilometer. Each computer monitors all transmissions, looking for packets containing its identifier as the destination. Only one signal may be present on the channel at a time and no single computer controls transmissions. Several upper layer protocols, such as DECnet and

TCP/IP use Ethernet as an underlying transport mechanism. Ethernet is to be contrasted with other data link protocols such as token ring, DDCMP or SDLC. Uses CSMA/CD.

Event logs: Event Logs are the logfiles saved by the Windows operating systems. Usually there are several Event Logs auditing a variety of events from different services of Windows. The creation of certain Event Logs is turned on by default but can be disabled by the user. The default storage location for Windows XP machines is: C:\Windows\system32\config*.evt, for Windows Vista/7 machines it is: C:\Windows\system32\Winevt*.evtx

EXIF metadata: Exchangeable image file format (Exif) is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. Typically there is a lot of information to find in the EXIF metadata, e.g. time, date and place of when and where a photograph has been taken and which camera model with which configuration was used.

EXT4: or **fourth extended filesystem** is a journaling file system for Linux, developed as the successor to EXT3.

External hard drives: External hard drives are a kind of external storage media. Modern external hard drives consist of a chassis, that offers connectivity via USB, Firewire, eSATA and/or Thunderbolt, and a regular 2,5” or 3,5” hard disk or SSD that is residing inside the chassis. Typically external hard drives can store a larger amount of data compared to USB thumbdrives or SD cards.

F

Faraday isolation bags: A dimensionless unit of electric charge quantity, equal to approximately 6.02 x 10 electric charge carriers. This is equivalent to one mole, also known as Avogadro´s constant. Faraday isolation bags are used to prevent mobile phones and devices from connecting to communication signals

FAT (File Allocation Table): is the name of a computer file system architecture and a family of industry standard file systems utilizing it. The FAT file system is technically relatively simple yet robust. It offers reasonably good performance even in light-weight implementations and is therefore widely adopted and supported by virtually all existing operating systems for personal computers. This makes it a well-suited format for data exchange between computers and devices of almost any type and age from the early 1980s up to the present.

File extension: File label usually 3 characters in length, preceded by a decimal point, that identifies the format of the data file or the application used to modify it.

FireBug: integrates with Firefox to put a wealth of development tools while browsing. It allows the user to edit, debug, and monitor CSS, HTML and JavaScript live in any web page.

FireWire: A high-speed serial bus that allows for the connection of up to 63 devices. Widelz used for downloading video from digital camcorders to the computer.

Flash cards: are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

Forensic Boot-DVDs: Forensic Boot-DVDs are DVDs that are bootable and contain an operating system containing software to perform digital forensics tasks. Besides just offering the forensic tools these Boot-DVDs take measures to prevent unintended write operations to any of the attached storage media.

Forensic copy: An exact copy (bit by bit) of the unit of storage of an IT system used in a forensic investigation.

FQDN (Fully Qualified Domain Name): sometimes also referred as an *absolute domain name*, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone. A fully qualified domain name is distinguished by its unambiguity; it can only be interpreted one way.

Fragmented data: Fragmented data is active data that has been divided and stored in different physical locations on the hard disk.

FTK Imager: FTK Imager is a multi-purpose software by Access Data Inc. It is free of charge and is capable of imaging, verifying, converting and mounting hard-discs and image files. FTK Imager can be downloaded at the following website: http://accessdata.com/support/adownloads

FTP (File Transfer Protocol): Protocol of the internet that allows transfer of files / data between computers connected via the internet.

Fiber optics: a high speed channel for transmitting data. Made of high-purity glass sealed within an opaque tube. Much faster than conventional copper wire such as coaxial cable.

Field: usually the smallest data element in a record; a specified area used for a particular category of data; for example, columns used to represent a particular item of data, such as an employees wage (fixed field). The particular field is always used to record the same kind of information. In free field records, each field has an identifier that is present in the record and linked to the contents of the field.

File: a collection of any form of data that is stored beyond the time of execution of a single job. A file may contain program instructions or data, which may be numerical, textual or graphical information.

File format: the type of file, such as picture or text; represented as a suffix at the end of the filename (text = TXT or .txt, etc.).

File server: a computer designated to store software, courseware, administrative tools, and other data on a local- or wide-area network. It "serves" this information to other computers via the network when users enter their personal access codes.

Folder: a place where a user's e-mail messages may be stored. Every user has a folder for new messages, and on most systems may create other folders for specific purposes.

Font: a set of consistent size, shape or style of printer characters, including alphabetic and numeric characters and other signs and symbols.

Foreground: high-priority processing, usually for realtime activities, automatically given precedence, by means of interrupts, over lower-priority processing.

Fragment: partial packet caused by a collision.

Frame: a packet sent over a serial link.

Freeware: software that is distributed for free, with no license fee.

Frequency: a measurement of the number of electromagnetic waves that pass over a given point in a given period of time.

G

Google AdSense: is a program run by Google Inc. that allows publishers in the Google Network of content sites to serve automatic text, image, video, and rich media adverts that are targeted to site content and audience. These adverts are administered, sorted, and maintained by Google, and they can generate revenue on either a per-click or per-impression basis.

GPS: The GPS (Global Positioning System) is a "constellation" of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from 100m to 10m for most equipment. GPS devices can provide information on previous travel via destination information, way points, and routes.

Gateway: an electronic door between one computer network and another. A device or set of devices that connects two or more networks, enabling data transfer between them. When the networks are similar, a gateway routes packets or messages. When the networks differ, a gateway also performs extensive protocol conversion.

GIF: Graphic Interchange Format. Specific format for low-resolution, compressed graphics interchange.

Gopher: a client program available via the Internet that allows users to review and retrieve information on other host systems via easy-to-use menus.

Graphic: a computer-generated picture produced on a computer screen or paper, ranging from simple line or bar graphs to colorful and detailed images.

Groupware: software that serves the group and makes the group as a whole more productive and efficient in group tasks. Example: Group Scheduling.

GUI: Graphical User Interface. Defines a format for scroll bars, buttons, menus, etc., and how they respond to the user.

H

Hacker: Person that has a thorough knowledge of the functionality of computers and networks that enables them to take advantage of the errors and failures in security of said systems.

Hard disk: Metal disk covered with a ferromagnetic burning layer. Making an analogy with a vinyl disc, the flat sides of the disc are the burning layer, the arm of the turntable is the laser arm and the needle on the turntable arm is the laser beam that reads / writes the information. A user can write, delete or re-write on magnetic disks as with audio tape.

Hard drives: Hard drives are the major storage device within computer systems. They consist of a circuit board, data and power connections, along with internal magnectically charged, ceramic, metal or glass platters that store the data. It is not unusual to discover hard drives that are not connected to or installed in a computer system.

Hardware: The physical components that make up a computer system such as the keyboard, monitor and mouse.

Hoax: Term used to define false rumours, especially about non-existent viruses spread over the network. Sometimes they are very successful and cause as much damage as a real virus.

Hosting providers: An **Internet hosting service** is a service that runs Internet servers, allowing organizations and individuals to serve content to the Internet. There are various levels of service and various kinds of services offered. A common kind of hosting is web hosting. Most hosting providers offer a combined variety of services. Web hosting services also offer e-mail hosting service, for example. DNS hosting service is usually bundled with domain name registration.

HTML code (Hypertext Markup Language): Language used for writing documents for web servers. HTML is an application from ISO Standard 8879:1986.

HTTP (Hypertext Transfer Protocol): HTTP is a protocol with the necessary agility and velocity to distribute and handle multimedia information systems over the internet. A characteristic of HTTP is the independence in the visualisation and representation of the data, allowing systems to be constructed independently of the development of new advances in the representation of data.

HTTPs: Secure HTTP protocol. The 2 principal characteristics are the coding and authentication. By means of the coding, the content of the communication of the server to the third party is concealed. The authentication allows users know that the server is bonafide with the use of certificated signatures by Certification of Authority.

Handshaking: a procedure performed by modems, terminals, and computers to verify that communication has been correctly established.

Hang: when a computer freezes, so that it does not respond to keyboard commands, it is said to "hang" or to have "hung."

Hard copy: a printed copy of machine output in a visually readable form.

Hardware: physical computer equipment such as electrical, electronic, magnetic and mechanical devices.

Hardwired: circuits that are permanently interconnected to perform a specific function, as distinct from circuits addressed by software in a program and, therefore, capable of performing a variety of functions, albeit more slowly. Also used to describe a non-switched connection between devices.

Header: the portion of a message, preceding the actual data, containing source and destination address and error-checking fields.

Host: a computer that is made available for use by multiple people simultaneously.

Host computer: in the context of networks, a computer that directly provides service to a user. In contrast to a network server, which provides services to a user through an intermediary host computer.

Hub/Hubs: A place of convergence in a network where data arrives from one or more directions and is forwarded out in one or more other directions. It usually works as a multiport repeater by generating a number of identical outputs from a single input (output=input). A hub may include a switch of some kind (adapted from).

Hyperlinkb: a pointer that when chosen displays the item to which it points. It typically takes the form of a button or highlighted text that point to related text, picture, video, or audio. Hyperlinks allow non-linear exploration of media that contain them.

Hypermedia: media (such as text, graphics, video, audio) that contains hyperlinks.

Hypertext: a document which has been marked up to allow a user to select words or pictures within the document, click on them, and connect to further information. The basis of the World-Wide Web.

I

I ROM memory: ROM stands for *Read-Only Memory*. The memory of the semiconductor that cannot be overwritten and maintains stored information intact, including in the case of loss of power supply. ROM is used to storing the system configuration or the programme from the boot-up of the computer.

ICQ: is an instant messaging computer program, which was first developed and popularized by the Israeli company Mirabilis, then bought by America Online, and since April 2010 owned by Mail.ru Group. The name *ICQ* is a homophone for the phrase "I seek you". This is an adaptation of the Morse code callout "CQ", which means "calling any station".

IMAP: Internet Message Access Protocol. An Internet service based on a standardized protocol for retrieving and/or accessing e-mail messages from the mail server (i.e., IMAP server).

Infrared: Infrared wireless technology is used for short- and medium-range communications and control in a variety of applications (e.g., wireless local area networks, links between notebooks and desktop computers, cordless modems, intrusion detectors). Infrared refers to energy in the region of the electromagnetic radiation spectrum at wavelengths longer than those of visible light, but shorter than those of radio waves.

Interface "Gnome": Is the core user interface of the GNOME desktop environment used by a variety of different Linux distributions. It provides basic functionality like switching between windows and launching applications. It replaces GNOME Panel and other software components from GNOME 2 to offer a user experience that breaks from the previous model of desktop metaphor, used in earlier versions of GNOME.

Internet access: is the means by which individual terminals, computers, mobile devices, and local area networks are connected to the global Internet. Internet access is usually sold by Internet Service Providers (ISPs) that use many different technologies offering a wide range of data rates to the end user.

Internet Assigned Numbers Authority (**IANA**): is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. IANA is a department operated by the Internet Corporation for Assigned Names and Numbers, also known as ICANN.

Internet browsing history: Software that is designed to browse websites like Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, etc often save histories of websites that were visited by the users of a computer system. The main purpose of these history logfiles or databases is

to allow the user to easily choose websites that were visited recently or very often. For forensic examiners the internet browsing history saved by the browsers can be a valuable source for finding evidence.

Internet Service Provider (ISP): is an organization that provides access to the Internet. Internet service providers can be either community-owned and non-profit, or privately owned and for-profit.

Internet: Global network of data based on TCP/IP protocol that are utilised to interconnect computers and, as such, the transport of diverse services, the most popular being e-mail, web and FTP services.

IP address: Internet Protocol. The Internet standard protocol that provides a common layer over dissimilar networks, used to move packets among host computers and through gateways if necessary.

Chain of 4 numbers separated by decimal points that are used to represent and identify a computer on the internet. ISP's assign IPs automatically when we connect to the internet.

ISP (Internet Service Provider): Organisation that provides connection to the internet for computers that are dedicated lines or switches. A profit making entity that as well as providing access to the internet for individuals and / or legal entities, can offer services such as web hosting, web-design consultancy, integration of websites and intranets, etc.

IT system: An information system (IS) - or application landscape - is any combination of information technology and people's activities that support operations, management and decision making. In a very broad sense, the term information system is frequently used to refer to the interaction between people, processes, data and technology. In this sense, the term is used to refer not only to the information and communication technology (ICT) that an organization uses, but also to the way in which people interact with this technology in support of business processes.

Icons: on-screen pictures that symbolize various commands.

I/O: Input/Output. The part of a computer system or the activity that is primarily dedicated to the passing of information into or out of a central processing unit.

Inbox: the mailbox that holds incoming e-mail.

Index: a list of the messages contained in a conference or a mail folder. Indexes generally show the date of the message, its title (or subject), the name of the user who wrote it, and an indication (with a "*" marker) of whether you have read that message.

Information hiding: a technique by which the structure and precise usage of information and data is concealed. The information is private to its owning objects and accessible to all other objects only by sending a message to the owner. This is the basis of encapsulation.

Information server: a computer on the Internet which acts as a library of documents and files that users can download.

Input: as a verb, to enter information, instructions, text, etc. , in a computer system or program. As a noun, the data so entered. Input devices include the keyboard and OCR reader.

Instruction: a statement to the computer that specifies an operation to be performed and the values and locations of the data to be processed.

Interactive: pertaining to an application in which each entry evokes a response from a system or program, as in an inquiry system, for example, an airline reservation system. An interactive system may also be conversational, implying continuous dialog between the user and the system.

INTERNET: a concatenation of many individual TCP/IP campus, state, regional, and national networks (such as CSUNET, SUPERNET, WESTNET, NSFNET, ARPANET) into one single logical network all sharing a common addressing scheme. The global "network of networks" that connects huge corporations, small businesses, universities, and individuals. Every Internet user can send E-Mail to every other Internet user. Most Internet users can also read and post Netnews messages. In addition, many Internet users have access to more advanced services for information search and retrieval, such as Gopher, FTP, WWW, and WAIS.

IP Address: the numeric address of a computer connected to the Internet; also called Internet address.

Interrupt: a suspension of a process, such as the execution of a computer program, caused by an event external to the computer and performed in such a way that the process can be resumed. Events of this kind include sensors monitoring laboratory equipment or a user pressing an interrupt key.

IRC: Internet Relay Chat, or just Chat. An on-line group discussion.

ISDN: Integrated Services Digital Network. An international communications standard for a common interface to digital networks that allows the integration of voice and data on a common transport mechanism. Proposed by Bellcore for transmission of data, voice and higher-bandwidth technologies over phone lines.

ISO: International Standards Organization. International standard making body responsible for the OSI network standards and the OSI reference model.

J

JAVA: Java is a language oriented to objects and developed by Sun Microsystems. It shares similarities with C, C++ and Objective C. Basing itself on other object oriented languages, Java utilises the best parts of the others and eliminates the least effective points. The principal objective of Java was to make a language that had the capacity to be executed in a secure way across the internet (although the code was maliciously written). This characteristic requires the elimination of many C and C++ uses and constructions. The most important is that no pointers exist. In Java, the program cannot arbitrarily access memory addresses.

Job: a set of data that defines a unit of work for a computer; it usually includes all necessary computer programs, linkages, files and instructions to the operating system.

JPEG: Joint Photographic Experts Group. The ISO proposed standard for compression of digital data, especially 24-bit color images. It is lossy in that it reduces the file size at the expense of image quality. PostScript Level 2 color printers are supposed to be able to receive, decompress and print JPEG compressed images. Uses quantization and Huffman encoding.

Justify: in word processing, to print a document with even (straight, non-ragged) right and left margins.

K

Key: an identifier in a database or file. A primary key is a unique identifier. A secondary key is typically not unique. A key may be used to specify data in a query. Example: Tag number to specify a car in a database of automobile registration information.

Keyboard: similar to a typewriter, contains the letters for typing text, and keys that give the computer its commands.

Kilobyte(K): 1,024 bytes, often used to mean 1,000 bytes.

L

LACNIC (Latin America and Caribbean Network Information Centre): is the Regional Internet Registry for the Latin American and Caribbean regions. LACNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organisation whose members include Internet Service Providers, and similar organisations.

LAN: Local Area Network. A common name for the networking technologies standardized by the IEEE (Institute of Electrical and Electronics Engineers).

LAN CONFIGURATION: LAN topology such as Ethernet or token ring, or MAC addresses such as Ethernet address (MAC: Medium Access Control, a part of the data link layer in the OSI seven layer model).

Linux: is a Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the Linux kernel, an operating system kernel first released 5 October 1991 by Linus Torvalds.

Live computer system: A Live computer system is a computer system that is powered on.

Live data forensics: Live data forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Live data forensics follow this aim but is only focused on computer systems that are powered on. The main purpose is to acquire volatile data that would otherwise get lost if the computer system is turned off or would be overwritten if the computer system will stay turned on for a longer period.

Log: Register of determined events generated by the operating system, or application, about a given period of time. Logs can be used by external auditors for registering / reconstructing the use of the computer or application.

LTE networks: LTE Advanced is a mobile communication standard, formally submitted as a candidate 4G system to ITU-T in late 2009, was approved into ITU, International Telecommunications Union, IMT-Advanced and was finalized by 3GPP in March 2011.[1] It is standardized by the 3rd Generation Partnership Project (3GPP) as a major enhancement of the Long Term Evolution (LTE).standard.

Laser printer: an electro-photographic (xerographic) printer in which a laser is used as the light source.

Layer: a grouping of related tasks involving the transfer of information. Also, a level of the OSI (Open System Interconnection) reference model.

Line: in communications, a wire connecting a terminal to a computer; also a unit of text.

Line printer: a computer output device in which an entire line of print is composed and determined within the printer prior to printing. The line is printed as a unit and there is no movement of a print head.

Link: a form of markup which designates that data within a document will automatically connect with either nested data or an outside source. Used in the design of hypertext.

LISTSERV: A server that manages named lists of recipients and files and access-controls for them. Accepts commands by interactive message or electronic mail. A note sent to a list name is resent to each recipient in the list. Will send a copy of a file on command.

Load: v. To transfer a program held on some external storage medium (such as magnetic tape or disk) into the main memory of the machine in a form suitable for execution.

Login or logon: the opening sequence of keystrokes used via computer screen instructions to connect to a system or begin operations on a computer.

Login ID: same as account name or user ID.

Logoff: leave a network system, usually by typing "bye" or "q" for quit. Sometimes called "logout."

M

MAC address (Media Access Control): Also known as the hardware address or Ethernet address. A unique identifier specific to the network card inside a computer. Allows the DHCP server to confirm that the computer is allowed to access the network. MAC addresses are written as XX-XX-XX-XX-XX-XX, where the Xs represent digits or letters from A to F.

Mac OS: is a series of graphical user interface-based operating systems developed by Apple Inc. (formerly Apple Computer, Inc.) for their Macintosh line of computer systems. The Macintosh user experience is credited with popularizing the graphical user interface. The original form of what Apple would later name the "Mac OS" was the integral and unnamed system software first introduced in 1984 with the original Macintosh, usually referred to simply as the **System** software.

Macro virus: Ultimate presentation of the virus. They are transported in application files (Word, Excel, etc.) and not in binary files (how traditional viruses are). They are executed on the opening of the data file in which they are contained.

Mainframe computers: An industry term for a large computer, typically manufactured by a large company such as IBM for the commercial applications and other large-scale computing purposes.

Malware: Malicious software. Any programme whose objective is to cause damage to computers, systems or networks and, as a result, to its users.

Memory cache: A type of memory that temporarily stores information that is used frequently to enable rapid access to this data.

Memory cards: are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

Memory devices: A memory device is any device that is capable of storing data either permanently or non-permanently.

Metadata: Metadata is information about a combination of files and / or folders that can describe, for example, how and when it was created, received, accessed and modified and by whom. This data is utilised in Computer Forensics to reconstruct the chain of events associated to the analysed file. Depending on the context in which the term is employed, it can refer to one piece of data or another.

Microprocessors: incorporates the functions of a computer's central processing unit (CPU) on a single integrated circuit, (IC) or at most a few integrated circuits. It is a multipurpose, programmable device that accepts digital data as input, processes it according to instructions stored in its memory, and provides results as output. It is an example of sequential digital logic, as it has internal memory. Microprocessors operate on numbers and symbols represented in the binary numeral system.

Microsoft PubCenter is a publisher's ad serving application developed by Microsoft in addition to Microsoft adCenter, which allows advertisers to place ads on search engines as well as select MSN websites or applications. Currently, in its beta version.

Microsoft Windows is a series of graphical interface operating systems developed, marketed, and sold by Microsoft.

Minicomputers: is a term for a class of smaller computers that evolved in the mid-1960s and sold for much less than mainframe and mid-size computers from IBM and its direct competitors.

Modem: MOdulator/DEModulator. A device used by computers to communicate over telephone lines. It is usually recognized by connection to a phone line, but there are also cable modems based on the DSL technology (e.g., cable modems). Can be combined with a facsimile (fax) functionality within a PC card (adapted from).

Modular rack-mounted systems: Modular rack-mounted systems are computer systems that are hosted in a rack and often times are built in a modular way allowing each hardware module to be replaced instantly without having negative impacts on the whole system. These racks most usually can host multiple computer systems with 19” form factor.

Mozilla Firefox is a free and open source web browser developed for Microsoft Windows, Mac OS X, and Linux coordinated by Mozilla Corporation and Mozilla Foundation. Firefox uses the Gecko layout engine to render web pages, which implements current and anticipated web standards.

Machine language: a programming language or instruction code that is immediately interpretable by the hardware of the machine concerned.

Macro: a single computer instruction that stands for a given sequence of instructions.

Magnetic disk: a flat circular plate with a magnetic surface layer used for storage of data.

Magnetic tape: a tape with a magnetic surface layer on which data can be stored by magnetic recording.

Mailbox: a file of e-mail messages on which a UA can operate as if they were incoming messages (read, reply, forward, delete, etc). Compare with inbox.

MAILER: a BITNET MTA for VM/CMS that natively supports domain names and routing through gateways. It is supplied without charge to BITNET members by Princeton University.

Main memory: usually the fastest storage device of a computer and the one from which instructions are executed.

Mainframe: the cabinet that houses the central processing unit and main memory of a computer system, separate from peripheral devices such as card readers, printers, disk drives, etc. and device controllers. The term has come to be applied to the computer itself in the case of large systems. A large computer system; the IBM ES9000.

Mainframe, minicomputer, micro-computer: three sizes of computers. Big corporations use mainframes and large school systems might use a mid-range computer, sometimes called a minicomputer, as a file server and administrative tool. The correct term for microcomputer is personal computer or PC.

MB: Megabytes. 1,048,576 bytes, often used to mean one million bytes (1,000,000) bytes.

Medium: the material used to support the transmission of data. This can be copper wire, coaxial cable, optical fiber, or electromagnetic wave as in microwave.

Memory: a device or medium that serves for temporary storage of programs and data during program execution. The term is synonymous with storage, although it is most frequently used for referring to the internal storage of a computer that can be directly addressed by operating instructions. Your computer's temporary storage capacity, measured in kilobytes (KB) or megabytes (MB) of RAM (random-access memory). Long-term data storage on discs, is also measured in kilobytes or megabytes.

Menu: a displayed list of options from which a choice can be made. The list is often displayed with a code opposite each option; the selection may be made by typing the appropriate code.

Message: E-Mail: The unit of information transferred by an e-mail system. It consists of an envelope that identifies the recipients to an MTA; headers containing who the message is from, to, subject, relaying information, etc; and a body that contains the information the sender wishes to communicate.

Method: a procedure whose code implements the behavior invoked by sending a message.

Module: a logically self-contained and discrete part of a larger computer program.

Monitor: a television-like screen that shows text, graphics, and other functions performed by the computer.

Mouse: a device that is moved by hand to move a pointer to indicate a precise position on a display screen. The device has one or more buttons on top and a cable connected to a computer; it may use wheels and be friction-driven or it may use light reflected from a special pad.

Multimedia: a single work assembled using elements from more than one medium, such as high-resolution color images, sounds, video, and text that contains characters in multiple fonts and styles.

Multimedia mail: provides the capability to compose, send and read messages that include things such as spreadsheets, line drawings, animated graphics, high-resolution color images, digitized speech, video, and WYSIWYG text that may contain characters in multiple fonts and styles, etc.

Multiuser: the capability of some computer systems to provide access to many simultaneous users.

N

Nesting: placing documents within other documents. Nesting allows a user to access material in a non-linear fashion - this is the primary factor needed for developing hypertext.

Network: a collection of two or more computers interconnected by telephone lines, coaxial cables, satellite links, radio, and/or some other communication technique. A computer "network" is a group of computers which are connected together and which communicate with one another for a common purpose. Computer networks support "people and organization" networks, users who also share a common purpose for communicating.

Network interface cards: Provides network connection (either with cable or wireless). Can be in the form of an expansion board or a PC card.

Nickname: a name that can be used in place of an e-mail address. Same as alias.

Node: a member of a network or a point where one or more functional units interconnect transmission lines.

NTFS (New Technology File System): is a proprietary file system developed by Microsoft Corporation for its Windows line of operating systems, beginning with Windows NT 3.1 and Windows 2000, including Windows XP, Windows Server 2003, and all their successors to date.

O

Off-line: not connected to a network. You can save money on pay-for-use networks by preparing your messages off-line using your word-processing software, and uploading them instead of typing them in while you're connected to (or on-line with) the network.

On-line: active and prepared for operation. Also suggests access to a computer network. Connected to a network or via a network. Examples: Send me a message on-line. In other words, send me an e-mail message.

Online service provider: can for example be an internet service provider, email provider, news provider (press), entertainment provider (music, movies), search, e-shopping site (online stores), e-finance or e-banking site, e-health site, e-government site, Wikipedia, Usenet. In its original more limited definition it referred only to a commercial computer communication service in which paid members could dial via a computer modem the service's private computer network and access various services and information resources such a bulletin boards, downloadable files and programs, news articles, chat rooms, and electronic mail services.

Open: under open systems, unencumbered specifications are freely available, independent branding and certification processes exist, multiple implementations of a single product may be created and competition is enhanced.

Open platform: a national Internet network that would allow citizens the ability to access, create, and publish information.

Open system: a system that implements sufficiently open specifications for interfaces, services and supporting formats to enable properly-engineered applications software to be ported with minimal changes across a wide range of systems, to interoperate with other applications on local and remote systems, and to interact with users in a style that facilitates user portability.

OSI: Open Systems Interconnect. An international standard suite of protocols defined by International Standards Organization, that implements the OSI reference model for network communications between computers.

Open Windows: a windowing environment from Sun Microsystems based on X-windows and NeWS.

Operating system (OS): software that controls the basic, low-level hardware operations, and file management. It is provides the link between the user and the hardware. Popular operating systems include: DOS, MacOS, VMS, VM, MVS, UNIX, and OS/2. (Note that "Windows 3.x" is not an operating system as such, since in must have DOS to work).

Output: information retrieved from a computer, displayed by a computer or produced by a program running on a computer.

P

P2P-Peer to Peer: Protocol that uses the internet for the interchange and download of files. The term P2P comes from *peer-to-peer* and refers to a network of equals, meaning that the status of each client is the same. The existence of servers in the practical application of the P2P networks is due to the fact that its clients do not possess fixed IP addresses. As a consequence these servers only offer a listing of clients and file searches.

Pagers: A pager is a device that may be used for sending and receiving electronic messages, numeric (e.g., phone numbers) and alphanumeric (text, often including e-mail)

Parallel port dongle: A small device with a parallel port connector that may provide programmable memory, remote update, lease control algorithms or counters.

Partitions: is the act of dividing a hard disk drive into multiple logical storage units referred to as *partitions*, to treat one physical disk drive as if it were multiple disks. Partitions are also termed "slices" for operating systems based on BSD, Solaris or GNU Hurd. A partition editor software program can be used to create, resize, delete, and manipulate these partitions on the hard disk.

Peripheral Devices: are not an integral part of the computer but connect to it to improve its capabilities. Examples of peripheral devices are: scanners, printers, tape drives, webcams, loudspeakers, microphones, fax , answering machines and card readers.

Personal Digital Assistant (PDA): A small (i.e., pocket-sized) device that can include computing, telephone/fax, paging, networking, and other features.

PGP: Pretty Good Privacy. Freeware cryptography software (see, e.g., www.pgpI.org) originally developed by Philip R. Zimmermann in 1991. Can be used to encrypt/sign e-mails or encrypt computer files. There is also a low-cost commercial version.

Pharming: A technique with the same objective as *Phishing*, but is not based on misleading the user but the Domain Named System (DNS) instead. In this way, if the user's ISP utilizes vulnerable DNSs, the "pharmer" redirects all the traffic of the URLs that are of interest, to the servers under his/her control. These have an identical appearance to the originals. The only way to detect this type of attack is through the certified servers that, in the case of the "pharmer", will not have a Certification of Authority.

Phishing: Technique of deception that combines social engineering with certain technical tricks with the objective of stealing personal banking information from an individual user. *Phishing* attacks

cleverly take the appearance of e-mails from a trusted entity requesting bank details or passwords of the user.

Phreaker or Phreak: IT pirate specialised in using telephone networks to access other people's systems or often just to avoid paying telephone bills. The techniques used by *Phreakers* are commonly known as *phreaks*.

Programme pirating: Activity of copying, distributing or using existing IT programmes, infringing legally upon the intellectual property rights that protect its authors.

POP3: Post Office Protocol. An Internet service based on a standardized protocol for retrieving e-mail messages from the mail server (i.e., POP server).

Port replicators: A device containing common PC ports such as serial, parallel, and network ports that plugs into a portable computer. A port replicator is similar to a docking station, but docking stations normally provide capability for additional expansion boards.

Portable media players: store and play digital media such as music and other audio, images, video as well as other files including documents and other types of fields that are capable of being stored digitally.

Proxy: In computer networks, a **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control their complexity. Today, most proxies are **web proxies**, facilitating access to content on the World Wide Web.

Packet: basic component of communication over a network. A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a complete whole through a network. It contains source and destination address, data and control information. See also frame.

Parameter: a variable, or quantity that can assume any of a given set of values, of which there are two kinds: formal and actual. (See argument.)

Password: a string of characters that a program, computer operator, or user must supply to meet security requirements before gaining access.

Peripheral: anything extra or added on for your computer, such as a modem, a mouse, or a fax adapter. Peripherals can be added on externally or installed inside the machine.

PC: Personal Computer. An IBM or IBM clone personal computer (Microcomputer) that is used by one person, as opposed to a Macintosh.

Ping: slang term for a small network message (ICMP ECHO) sent by a computer to check for the presence and aliveness of another.

To verify the presence of. To get the attention of.

Pixel: Picture Element. In computer graphics, the smallest element of a display space that can be independently assigned color or intensity.

Platform: hardware environment that supports the running of a computer system.

Port: that portion of a computer through which a peripheral device may communicate. Often identified with the various plug-in jacks on the back of your computer. On a network hub, it is the connector that receives the wire link from a node.

Portable: in computer usage, a file or program is "portable" if it can be used by a variety of software on a variety of hardware platforms. Numeric data files written as plain character format files are fairly portable.

Post: the act of placing a message in an on-line conference. The noun "posting" is sometimes used to refer to a conference message.

Printer: an output device that converts the coded information from the processor into a readable form on paper.

Printout: the printed output of a computer.

Procedure: a portion of a high-level language program that performs a specific task.

Process: a systematic sequence of operations to produce a specified result; a unique, finite course of events defined by its purpose or by its effect and achieved under given conditions. As a verb, to perform operations on data in a process. Also an address space and the code executing in it.

Program: a set of actions or instructions that a machine is capable of interpreting and executing. Used as a verb, to design, write and test such instructions.

Programmer: a person who designs, write and tests computer programs.

Programming: a notation for the precise description of computer programs or algorithms. Programming language languages are artificial languages in which the syntax and semantics are strictly defined.

Prompt: a character or message provided by an operating system or program to indicate that it is ready to accept input.

Protocol: an agreement that governs the procedures used to exchange information between cooperating entities and usually includes how much information is to be sent, how often it is sent, how to recover from transmission errors and who is to receive the information.

Public domain: not protected by copyright; you may freely make copies and distribute them; you may make derivative works.

Q

Query: a request that specifies the manner in which data is to be extracted from one or more databases.

Queue: a sequence of stored computer data or programs awaiting processing that are processed in the order first-in first-out (FIFO).

Quit: ends the work without writing out a new file or new version of the exiting work file unless there is a save that interrupts before dumping the session.

Qwerty: is the most common modern-day keyboard layout.

R

RAID: Redundant Array of Inexpensive Disks. A way of creating a fault-tolerant storage system. There are 6 levels. Level 0 uses byte-level striping. Level 1 uses mirroring. Level 2 uses bit-level striping. Level 3 stores error correcting information (such as parity) on a separate disk, and uses data striping on the remaining drives. Level 4 is level 3 with block level striping. Level 5 uses block level and parity data striping.

RAM memory: RAM stands for *Random Access Memory.* RAM memory temporarily stores data that the computer is working with. This memory loses its content as a result of a power loss.

Recovered data: The term that identifies recovered or reconstructed files or folders that had been deleted from the active data area. These files can be recovered with the original size and format or in small fragments that will require a forensic reconstruction task.

Refusal of service: Incident where a user or an organisation are refused access to a resource they can normally use. Usually, the loss of access is due to the unavailability of a particular network service, such as e-mail, or the temporary loss of all network connections and services. In the worst case, for example, a website where millions of people access can be forced temporarily to cease operating. Although, normally intentional and malicious these type of attacks sometimes occur accidentally. If these attacks do not always result in the theft of information, they almost invariably cost a lot of time and money to the person or organisation affected.

Reverse engineering: Consists of the analysis of the binary code of a programme or application to determine its behaviour.

RIPE Réseaux IP Européens (RIPE, French **for "European IP Networks"):** is a forum open to all parties with an interest in the technical development of the Internet. The RIPE community's objective is to ensure that the administrative and technical coordination necessary to maintain and develop the Internet continues. It is not a standardisation organisation like the IETF and does not deal with domain names like ICANN.

Routers: is a device that determines the next network point that a packet should be forwarded towards its destination. It must be connected to at least 2 networks. It is intelligent and works on routing tables. Although it is located at the gateway to a network it does not necessarily have to be the networks gateway to the Internet.

Random access: differs from direct access by the fact that each element can be accessed with the same ease and speed as any other.

Real time: the processing of transactions as they occur rather than batching them. Pertaining to an application in which response to input is fast enough to affect subsequent inputs and guide the process and in which records are updated immediately. The lag from input time to output time must be sufficiently small for acceptable timeliness. Timeliness is a function of the total system: missile guidance requires output within a few milliseconds of input, scheduling of steamships requires response time in days. Realtime systems are those with response time of milliseconds, interactive system in seconds and batch system in hours or days.

Record: a collection of related data or words, treated as a unit. For example, in stock control, each invoice could constitute one record.

Record length: depending on the context, the length in bytes (i.e., columns) of a physical record or a logical record. On ICPSR Tape Information Forms and on CDNet, the abbreviation "RecLen" is used for physical record length.

Record type: a record that has a consistent logical structure. In files that include different units of analysis, for instance, different record types are needed to hold the different variables. For example, one record type might have a variable for income in one column and another record type might have a variable for household size in that same column. The codebook will describe these different structures and how to determine which is which so that you can tell your statistical software how to interpret that particular column as income or household size.

Recovery: the process by which data bases are rebuilt after a system fails.

Relational database: an organization of data into tables with each column containing the values of a data element and each row representing a record.

Remote: equipment or site that is located out of the way or at a distance from primary equipment or a larger or primary site. Sometimes used as the opposite of local.

Remote access: the ability to access a computer from outside a building in which it is housed. Remote access requires communications hardware, software, and actual physical links, although this can be as simple as common carrier (telephone) lines or as complex as TELNET login to another computer across the Internet.

Resource: an on-line information set or an on-line interactive option. An on-line library catalog or the local school lunch menu are examples of information sets. On-line menus or graphical user interfaces, Internet e-mail, on-line conferences, telnet, FTP, and Gopher are examples of interactive options.

Response: a message placed in a conference as a follow-up to a topic or to another response; or, a reply to an e-mail message.

Reuse and re-usability: an approach to software engineering that emphasizes reusing software assets, including designs and code, and building software assets likely to be re-usable in future applications.

ROM: read-only memory. Information is stored once, usually by the manufacturer, that cannot be changed. Most compact discs are ROM.

Root directory: the directory that contains all other directories.

Router: a device connecting separate networks that forwards a packet from one network to another based only on the network address for the protocol being used. For example, an IP router looks only at the IP network number.

Routine: part of a computer program, or a sequence of instructions called by a program, that may have some general or frequent use.

Routing: the process of finding a path over which a packet can travel to reach its destination.

Run: the single, continuous execution of a program by a computer on a given set of data. As a verb, to initiate processing by a program.

S

Scheduler: is the method by which threads, processes or data flows are given access to system resources (e.g. processor time, communications bandwidth). This is usually done to load balance a system effectively or achieve a target quality of service. The need for a scheduling algorithm arises from the requirement for most modern systems to perform multitasking (execute more than one process at a time) and multiplexing (transmit multiple flows simultaneously).

SHA-256 hash: is a set of cryptographic hash functions (**SHA-224, SHA-256, SHA-384, SHA-512**) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.

Slack area data: Due to the necessity of the computer to assign fixed sized blocks of disk space, there exists an area at the end of every file that, despite being assigned to the file, contains information not relating to the other information contained therein. This area is called "slack" and contains information of the contents that were on this block space before it was assigned a new file.

Slack space: Slack space is an area of space on a storage devices that is allocated to a certain unit, e.g. a file, a partition, a disk, an MFT record but is not used by this unit. Oftentimes a forensic specialist can find data belonging to formerly stored files in these slack spaces. If for example a cluster gets allocated to a newly created file but the data of this file do not use the whole cluster than there is a good chance to find traces of a previously stored file in the slack space of the cluster.

Social Engineering: Techniques or skills that allow manipulation of a person that, voluntarily carries out actions that they normally would not do, such as the revealing of information.

Software: Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Website development, file management, or inventory management.

Solid state disks: they store information in a different way than hard disks, while intending to provide access in the same way as tradtional hard disks. Whereas hard disks store data on platters, solid state disks store data using microchips that have no moving parts. As such they are less likely to be damaged by shock and they offer faster access to the data. These devices may hold valuable evidence.

Speaker magnets: Common speakers consist of a magnet, a coil and a cone. The speaker magnet is there to provide a permanent magnetic field for the the speaker coil, which is embedded in the paper of the speaker cone. When the audio signal flows throw the speaker coil it generates a small magnetic

field the strength of which varies with the strength of the audio signal. This small magnetic field is repelled by or attracted to the permanent magnetic field produced by the speaker magnet.

Storage devices: is a device for recording (storing) information (data). Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs.

Scanner: a device that senses alterations of light and dark.

Scheduling: an automated capability to schedule meetings and/or resources (such as meeting rooms, projectors, etc.) by looking at online calendars.

Screen: the surface of a monitor on which information can be viewed.

Screen editor: a program that allows a file to be edited by making changes to the text displayed on the screen. It may also support commands to make changes to the whole file at once. Changes to the portion displayed on the screen are immediately shown.

Scroll: to move all or part of the display image vertically or horizontally to view data otherwise excluded. Scrolling can be performed with a mouse in the horizontal/vertical bars on each window or by using the page up/down - home/end - or arrow keys.

Segment: a section of network wiring. Segments are connected by repeaters, bridges or routers.

Sequential: a method of storing and retrieving information that requires data to be written and read sequentially. Accessing any portion of the data requires reading all the preceding data.

Server: a computer that shares its resources, such as printers and files, with other computers on the network. An example of this is a Network Files System Server which shares its disk space with a workstation that does not have a disk drive of its own.

Service (or service provider): an organization that provides access to part of the Internet. You have to arrange for an account with a service to connect your computer to the Internet.

Session: networking term used to refer to the logical stream of data flowing between two programs and being communicated over a network. There may be many different sessions emanating from any one node on a network.

Shareware: protected by copyright; holder allows you to make and distribute copies under the condition that those who adopt the software after preview pay a fee to the holder of the copyright; derivative works are not allowed; you may make an archival copy.

Shell: a term that usually refers to the user interface of an operating system. A shell is the command processor that is the actual interface between the kernel and the user. The C shell or the Bourne shell are the primary user interfaces on UNIX systems. Contrasts with the kernel, which interacts with the computer at low levels.

Simulation: an imitation of the behavior of some existing or intended system, or some aspect of that behavior. Examples of areas where simulation is used include communications network design, weather forecasting and training. Physical systems can also be simulated, for example, chemical or nuclear reactions.

Software: computer programs that perform various tasks. Word processing programs (like WordPerfect or Microsoft Word), spreadsheet programs (like Lotus or Excel), or database programs (like dBase III+, Foxbase, or FileMaker) are all software.

Software tool: a program that is employed in the development, repair or enhancement of other programs. Tools include editors, compilers and linkers. Also refers to utilities, such as formatters and file utilities.

Source code: the program in a language prepared by the programmer. This code cannot be directly executed by the computer and must first be translated into object code.

Spreadsheet: software program that allows mathematical calculations, such as budgeting, keeping track of investments, or tracking grades.

SQL: Structured Query Language. ANSI standard data manipulation language used in most relational data base systems. A language for requesting data from a relational database.

Storage: a device or medium that can retain data for subsequent retrieval.

String: a sequence of characters.

Striping: disk striping copies blocks, bytes or bits across multiple disks in such a way that if one disk is lost, the data can be created using the blocks or bits on the remaining disks.

Surfing: net speak for wandering, whether one is surfing through cable stations or surfing the Internet.

T

Tablet Devices: A tablet computer is a device that is operated by touching the screen rather than using a keyboard or mouse. It is normally larger than a mobile phone or **Personal Digital Assistant**

Traceable: Traceability refers to the completeness of the information about every step in a process chain. The formal definition of traceability is the ability to chronologically interrelate uniquely identifiable entities in a way that is verifiable. Traceability is the ability to verify the history, location, or application of an item by means of documented recorded identification.

TrueCrypt: is a free software application used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or (under Microsoft Windows except Windows 2000) the entire storage device (pre-boot authentication).

Trusted Platform Module (TPM): Most commonly the concept of TPM is applied in a TPM cryptoprocessor, known as TPM chip. This chip which is responsible for carrying out the TPM tasks is soldered to the mainboard of a computer system. The primary scope of a TPM is to assure the integrity of a platform. In this context "integrity" means "behave as intended" and a "platform" is generically any computer platform: Start the power-on boot process from a trusted condition and extend this trust until the OS has fully booted and applications running. TPM is also oftentimes used in combination with disk encryption, e.g. Truecrypt or Bitlocker Full Disk Encryption where it is used to protect the keys used to encrypt the computer's hard disks and provide integrity authentification for a trusted boot pathway.

Task: a separately dispatchable function on a computer.

TCP/IP: Transmission Control Protocol/INTERNET Protocol. The communication protocols on which the Internet is based.

TELNET: a program that allows users on the Internet to log in to remote systems from their own host system.

Terminal: a device connected to a computer network that acts as a point for entry or retrieval of information. Personal computers can be made to act as network terminals, by running terminal emulation (communication) programs.

Terabyte: 1,099,551,627,776 bytes, often used to mean one trillion bytes (1,000,000,000,000).

Time out: what happens when two computers are talking and one fails to respond within a certain time, for whatever reason.

Token ring: a LAN and protocol in which nodes are connected together in a ring and communication is controlled by a special packet called a token that is passed from node to node around the ring. A node can send data only when it receives the token and the token is not in use. Data is sent by attaching it to the token. The receiving node removes the data from the token.

Topic: in a conference, a message which is generally written to convey a new idea or a new piece of information, relevant to that conference.

Transfer: to copy or move information from one computer to another.

Transport Layer: the fourth layer of the OSI reference model. It provides transparent, reliable and cost-effective transfer of data.

Tree: a way of organizing information with general categories at the top, subcategories below, and narrower subcategories on a further level.

U

Ubuntu Linux: is a computer operating system based on the Debian Linux distribution and distributed as free and open source software, using its own desktop environment. It is named after the Southern African philosophy of ubuntu ("humanity towards others"). Ubuntu is designed primarily for use on personal computers, although a server edition also exists.

Universal Serial Bus (USB): is a standard that defines the protocols for communication, connection and power supply for devices that are to be connected to computers. Since its advent in the 1990s the number of devices that are now capable of being connected using this protocol has grown and new devices in all sorts of shapes and sizes are now used to store data.

Unix: is a multitasking, multi-user computer operating system originally developed in 1969.

Untrusted binaries: The term "untrusted binary" is most often used in conjunction with executable binary files that are stored or copied from an untrusted source. Any source that cannot be verified or has not undergone defined close validation procedures may potentially contain altered or even harmful source code and therefore should be considered untrusted. A typical example for untrusted binaries are executable files that are stored on a system other that the validated machine of the forensic specialist.

Unused or unassigned area data: Data that presently resides in the disk area that does not belong to a file; the remainder of the deleted digital documents.

URL(Uniform Resource Locator): A chain of characters which is assigned a unique address to each of the documents of the World Wide Web (*news, gopher*, etc.)

UTorrent: is a freeware, closed source BitTorrent client now owned by BitTorrent, Inc. It is the most widely used BitTorrent client outside China (where Xunlei is more popular). It gets the "µ" in its name from the SI prefix "micro-", referring to the program's small memory footprint: the program was designed to use minimal computer resources while offering functionality comparable to larger BitTorrent clients such as Vuze or BitComet. The program has received consistently good reviews for its feature set, performance, stability, and support for older hardware and versions of Windows.

Upload: to transfer information from a user's system to a remote system. Opposite of download.

User: anyone who uses a computer connected to the Internet.

User-friendly: a system or program that relatively untrained users can interact with easily.

Userid: a code that uniquely identifies a user and then provides access privileges to a computer system.

Username: account name or user ID.

Utility: a specialized program that performs a frequently required everyday task such as sorting, report program generation, or file updating.

V

Virtual: pertaining to a device or facility that does not physically exist, yet behaves as if it does. For example, a system with 4 megabytes of virtual memory may have only one megabyte of physical memory plus additional (slower and cheaper) auxiliary memory. Yet programs written as if 4 megabytes of physical memory were available will run correctly.

Virtual environment: The computational simulation of a work environment formed by the interconnection of multiple computers that permits the access to digital information independent of their physical location.

Virus: Programme that can infect other programmes, modifying them to include a copy of itself. Viruses basically have the function of propagation and replication but, furthermore, there are some that have harmful contents (*payload*) with different objectives, from a simple joke to causing serious damage to systems. These types of programmes can operate in various ways: Only notifying the user of its presence without causing apparent damage, Attempt to go unnoticed to cause the most damage possible or Take possession of the principal functions (to infect the filing system).

VoIP: Voice over Internet Protocol. The technology used to transmit voice conversations over a data network using the Internet protocol. Data network may be the Internet or a corporate Internet.

Volatile Data: Volatile Data are data that are digitally stored in a way that the probability is very high for their contents to get deleted, overwritten or altered in a short amount of time by human or automated interaction.

Volume: a physical unit of a storage medium, such as tape reel or disk pack, that is capable of having data recorded on it and subsequently read. Also refers to a contiguous collection of cylinders or blocks on a disk that are treated as a separate unit.

W

Warez: Pirate copies of programmes. Protected software versions that have had the protection removed.

Web Browser: A web browser can also be defined as an application software or program designed to enable users to access, retrieve and view documents and other resources on the Internet.

Windows Explorer: is a file manager application that is included with releases of the Microsoft Windows operating system from Windows 95 onwards. It provides a graphical user interface for accessing the file systems. It is also the component of the operating system that presents many user interface items on the monitor such as the taskbar and desktop. Controlling the computer is possible without Windows Explorer running (for example, the File | Run command in Task Manager on NT-derived versions of Windows will function without it, as will commands typed in a command prompt window).

Wireless Modems: A wireless modem is a type of modulator-demodulator which connects to a wireless network instead of using telephone or cable television lines. A mobile Internet user can connect using a wireless modem to a wireless Internet Service Provider (ISP) to get Internet access.

WireShark: is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named **Ethereal**, in May 2006 the project was renamed Wireshark due to trademark issues.

WLAN networks: wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

Word Processor: A software program used to turn the computer into a typewriter for wiring letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect, MS-Word.

Worm: IT programme that auto-duplicates and auto-propagates. In contrast with viruses, worms are usually written especially for networks. Network worms were first defined by Shoch & Hupp, of Xerox, in the magazine *ACM Communications* (March 1982). The first famous internet worm appeared in November 1988 propagated itself to more than 6,000 systems at large on the internet.

WWW (World Wide Web): The universe of network-accessible information, i.e., all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

Whois: the name of the nickname database that contains full name, postal address, telephone number, and network mailbox for registered users. Also the name of the local command to access this database, and the name of the protocol used by this command (RFC-954) that is now an elective draft standard.

Window: a rectangular area on a display screen in which part of an image or file is displayed. The window can be any size up to that of the screen and more than one window can be displayed at once.

Windows: a trademark of Microsoft Corporation for a software product that provides an environment for a graphical user interface for DOS and DOS applications.

Word processor: a program used to enter or edit text information in personal computers, often used to create a file before it is uploaded to a network; may also be used to process text after it has been downloaded.

Work space: disk space made available to the system to provide temporary storage space for files too large to fit within a user's permanent disk storage quota or for files not needed beyond a single run of a program or set of programs.

Workstation: a general purpose computer that is small enough and inexpensive enough to reside at a person's work area for his or her exclusive use. It includes microcomputers such as Macintosh, and PCs running DOS, as well as high-performance desktop and deskside computers.

Write: to record data in a storage device, a data medium, or an output display. To save information, especially files, to a disk, to replace old data with new and permit later access from within a software package; the complement of read.

Z

ZIP drives: A removable hard disk system. A ZIP drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. The trademarked ZIP drive was developed and is sold by Iomega Corporation. Zip drives and disks come in two sizes.

X

X window system: standard for controlling the display on a bitmapped terminal. X-windows normally uses a network connection, and unlike the typical terminal connection, multiple applications possibly on different computers can use the display simultaneously in different windows.

X-term: an X-windows client that provides a window for terminal emulation.

7. Compendium of Case law examples

To be gathered from various jurisprudences and presented as a separate appendix.

8. Conclusions

The Budapest Convention on Cybercrime Parties to the Convention are expected to enact law enforcement powers for securing electronic evidence and for enabling efficient international cooperation. Under Article 14 these powers can be applied to electronic evidence in *any* offence. These powers include:

- Expedited preservation of data at domestic (Article 16) and international (Article 29) levels, including the partial disclosure of traffic data (Articles 17 and 30);
- Search and seizure of stored computer data (Article 19);
- Real-time collection of traffic data and interception of content data at domestic (Articles 20 and 21) and international (Articles 33 and 34) levels;
- Rapid mutual assistance to access data in foreign jurisdictions (Article 31);
- Transborder access to data without the need for mutual assistance (Article 32).

Additional resources which are complementary to the material published in this Benchbook (Guide) includes also:

- The proposal for law enforcement training strategies prepared under CyberCrime@IPA;
- The judicial training concept prepared by the Council of Europe and the training materials developed under CyberCrime@IPA;
- The typology study on criminal money flows on the internet prepared by MONEYVAL and the Global Project on Cybercrime of the Council of Europe;
- The guidelines for law enforcement/internet service provider cooperation adopted at the Octopus Conference of the Council of Europe in 2008;
- The Guidance Notes on Computer System, Botnets, Transborder access, Identity Theft, DDOS attacks, Critical infrastructure attacks, Malware, Spam, Production order for subscriber information and Terrorism (Guidance Notes Number 1 to 11);
- The Octopus Cybercrime Community, a forum linking up the many hundred public and private sector cybercrime experts from all over the world.

These standards and tools are available at www.coe.int/cybercrime.

Criminals are predators and the mass use of digital media and Internet has provided new opportunities for them to perpetrate their crimes. They have evolved new strategies for traditional offences by exploiting these new channels of communication and novel categories of crime have evolved. Consequently, it is imperative for all those involved in the legal system to be familiar with the different forms of electronic evidence and to know how to deal with them.

Almost any crime these days is likely to involve an electronic device that has a memory or some form of programming. Even where the crime itself has not used such a device, the actions of the perpetrator may well have been captured or recorded on a CCTV camera or through a Global Positioning System (GPS) device on a phone or in a vehicle. The securing of electronic evidence through digital forensic examination and investigation has become the primary tool in bringing criminals to justice.

The development of the Internet and its applications has led to evidence being found not only on personal computer devices, but also on websites, social networks, in emails and chat rooms. The development of "cloud" computing (where applications and data are stored remotely across national boundaries in non-specific locations) means that it is more important than ever for potential electronic evidence to be processed according to tried and trusted principles and practice.

Having on mind that the aim of the investigation is to obtain all evidence with regard to the case subject and to pertain the ability to reproduce and explain procedure which led to the acquisition, Trial phase is the one in which all the quality or lack of quality of the acquired evidences will be shown.

Prosecutors and Judges are becoming more comfortable with the existence and admission of electronic evidence. In some jurisdictions, not only is it that digital evidence is explicitly allowed by the criminal justice legal framework, but there are references and definitions of computers, computer networks, software, hardware and data in substantive and procedural norms of aforementioned framework. Also, in some jurisdictions, computer data is defined as a movable object to which all legal rules for tangible items can be implemented (destruction, alteration, theft, alienation, exchange etc.).

Some legal opinions about digital evidence are considering it non usable because of the possibility for easy alteration and forgery what makes them highly disputable and thus non admissible evidence. Following that logic, questions about other evidence, more classic and known, can be asked as well. Forgeries of the paper documents are wide spread. Fingerprint forgery can be produced, also alteration of photographic, video and audio materials. Numbers of other examples how "classical" evidence can be changed are known as well. In that sense, digital evidence should not be observed as more volatile or unreliable, especially having on mind that as society, industry and technology advances, more and more of traces, facts and evidences are going to exist in digital form. Therefore, admissibility of the digital evidence as real evidence should not represent an issue in the contemporary Prosecution Office or Court, under the condition that procedures described in this guide are followed.

When we are considering cybercrime evidence in electronic form, some considerations should be applied, such as authenticity and reliability, completeness of the evidence, believability and proportionality.

Authenticity and reliability of the cybercrime evidence can be observed from the point of the origin as well, and it must be preserved throughout the whole digital forensic procedure. In that case forensic staff should have knowledge or/and pay attention to the existence of an authentic search and seizure

order (warrant) by Prosecutor or Judge, records of searched and seized places, items and taken actions, acknowledgement (if applicable) of a suspect or person in possession of seized items that records are authentic, photographic or video recordings from the place were search was conducted and other documents and measures in that sense, if required by the local jurisdiction. Authenticity of digital evidence is preserved only if digital forensic laboratory staff or expert witness continues with actions which are carefully organised, executed and recorded. Digital forensic process must not put in jeopardy this requirement.

Completeness of the evidence can also sometimes represent a difficult task since some parts of the evidence can be missing due to different factors and reasons and with or without influence of the suspect and other persons involved in the actual case. In such occasion expert witness should concentrate on best possible approach to the existing items and their contents in order to extract most comprehensive state of the facts, without distortion or biased approach.

Believability is in close connection with authenticity and reliability, but maybe more importantly, its relation with report writing must be underlined. This criterion should be carefully presented in the report with clear explanations, logical connections and trustable outcomes of procedures and conclusions as the results of the process. The Prosecutors and Judges should be ready to use forensic examiners or expert witnesses in this field. Verbal presentation of the findings and testing of the believability can occur. In such case, an examiner or expert witness should possess thorough knowledge of the report, procedures and concluded facts, which are going to be presented or additionally requested to be explained or clarified.

In that sense, an examiner or witness who is going to present and explain findings in court, or in Prosecutors office (if applicable), should have certain qualities for verbal presentation like fluency in communication and professional approach, bearing in mind that sitting Judge and all present parties in the courtroom will carefully listen and follow not only examiners words, but his appearance and overall impression as well.

Of course, proportionality is very much needed and expected. Needless to say, any kind of intrusion or coercion will most certainly open significant possibility for the demise of the case. Also, following good practices of the Rule of Law, facts and evidences which are in favour of defendant should be presented and made available to the defence as well.

Not many Prosecutors and even smaller number of Judges will feel comfortable with cybercrime evidence report and in many cases unconscious but natural reaction will be non-understanding of presented facts and language which will follow with possible number of question to be more thoroughly explained in person during expert testimony on the main trial.

With regards to the expert witness status it will vary from country to country. In some systems experts are engaged by the Prosecution and defence, in some systems they are Court appointed, and there is

number of mixed systems in which all parties and Court alike can appoint or hire expert in different stages of the proceeding.

However, it is a very likely scenario that expert witness coming from the forensics laboratory of the State Authority will be engaged by the Prosecution or Court order. This also means that defence is going to most probably engage expert witness of their own who will challenge most, if not all aspects of the previously mentioned expert and laboratory. This kind of the situation is becoming more and more present in contemporary Court Rooms and Forensic Laboratory experts must be aware and prepared for such possibility.

Alternative presentation methods are depending on the technical possibilities of the Court room, but not only in that case. Plea bargaining and, in some countries, growing popularity of "deferred prosecution", can lead to the presentations in Prosecution offices as well. In most of the countries Court and Prosecution rooms are not going to be equipped with hardware to support complex presentations. Thus said, expert must be prepared to present same quality of the evidence with less of the technical possibilities. Situations like this should be anticipated and certified mobile equipment for such presentations can be a useful option.

In conclusion, computer crime and digital evidence presentation stage as a goal and outcome of invested time and effort of the criminal investigation and examiners and its staff, in some countries digital forensic expert witnesses, should be always on mind of involved personnel. Established facts and evidences will serve for establishing of the material or substantive truth, depending on the legal system.

However, these facts are going to be used for adjudication of the criminal case, reaching justice and compensation of the victims. Not a light task and burden for anyone, but most certainly very important goal to be achieved, for which all involved professionals, especially Prosecutors and Judges, have a crucial and final determine role.

9. Appendix and Acknowledgments

- Convention on Cybercrime (ETS 185)

- Additonal Protocol to the Convention on Cybercrime concerning the criminalisation of acts of racist and xenophobic nature committed through computer systems (ETS 189)

- Explanatory Report to the Convention on Cybercrime

- T-CY Guidance Notes

- Council of Europe Electronic Evidence Guide 2017 edition

- GLACY+ Project

- C-PROC Office

- Council of Europe Action Against Cybercrime Resources

- http://www.math.utah.edu/~wisnia/glossary.html