CyberCrime@IPA

EU/COE Joint Project on Regional Cooperation against Cybercrime

Judicial training

Introductory course on cybercrime and electronic evidence for judges and prosecutors

Training manual and trainer guide – Version 1.0

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Strasbourg, France
5 April 2013

www.coe.int/cybercrime

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

Contents

1 Introduction

Given the reliance of societies worldwide on information and communication technologies, judges and prosecutors must be prepared to deal with cybercrime and electronic evidence. While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, this seems to have been less the case for judges and prosecutors. Experience suggests that in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world. Particular efforts are therefore required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation.

A concept to support such efforts has been developed by the Council of Europe under the Project on Cybercrime in cooperation with the Lisbon Network of judicial training institutions in cooperation with a multi-stakeholder working group in the course of 2009.

The purpose of the concept was to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training.

The objectives of a training concept for judges and prosecutors are:

- To enable training institutes to deliver initial and in-service cybercrime training based on international standards
- To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- To provide advanced training to a critical number of judges and prosecutors
- To support the continued specialisation and technical training of judges and prosecutors
- To contribute to enhanced knowledge through networking among judges and prosecutors
- To facilitate access to different training initiatives and networks.

Through the Joint Regional Project of the European Union and Council of Europe CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime)[1], the training institutions from the projects areas (Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo[*]) are supported to implement the training concept.

In this context, training materials are developed to be used by training institutions and a "Training of Trainers Programme" was carried out. This final version of the training pack takes into account the feedback received from the judges and prosecutors who participated

1 The European Union/Council of Europe Joint Project CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime) is aimed at strengthening the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime.

* All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo

in the "Training of Trainers programme" and delivered the course in their own training institutions. Furthermore the final version has been discussed by the members of working group on judicial training and the trainers in an event organized for this purpose.

2 General Overview

2.1 Aim of the Course

This course is designed to provide judges and prosecutors an introductory level of knowledge on cybercrime and electronic evidence. The course will provide legal as well as practical information about the subject matters and concentrate on how these issues impact on the day-to-day work of judges and prosecutors.

By the end of the course judges and prosecutors will have basic knowledge of:

- cybercrime and electronic evidence
- how judges and prosecutors can deal with them
- what substantive and procedural laws as well as technologies can be applied, and
- how urgent and efficient measures as well as extensive international co-operation can be taken.

The course will cover the following subjects:

- Introduction to cybercrime – trends and tools
- Technology involved in cybercrime
- Cybercrime as a criminal offence in domestic legislation
- Electronic evidence practice, procedure and legislation
- Procedural law/ investigative measures in domestic legislation
- International cooperation

2.2 Why is this training necessary

Judges and prosecutors play an important role in the investigation and adjudication of individuals or groups that have committed crimes. With the increase in the number of incidence of crimes that have an element of cybercrime or electronic evidence increases the need for judges and prosecutors to be properly trained to understand the nature of these crimes and to also be aware of the legislation and the instruments for international cooperation available to handle such cases..

Criminals and criminal groups in general do not limit themselves and their activities based on the country borders, cybercrime is one kind of crime that excludes the need of the offender to travel across these borders to commit a crime, thus making the investigation and the prosecution of the perpetrator much harder. This emphasises the need for improved international/regional cooperation as well as interagency cooperation when dealing with cases of cybercrime.

Cases of cybercrime often require a swift and very efficient international or regional cooperation, which would provide for a timely investigation and prosecution of the perpetrators. As result the training institutions should make the effort to include in their curriculum modules that contain instructions about the instruments of international

cooperation that can be used when investigating cybercrime cases including the use of the 24/7 points of contact, MLA, Judicial Cooperation Activity, Judicial Cooperation Platforms etc.

2.3 The curriculum

This curriculum is a basic tool to be considered by the training institutions when conducting training on cybercrime. The aim of this document is to focus on the establishment and production of standardised courses or modules that would be used in project countries/areas in the carrying out of the initial training for judges and prosecutors involved in adjudicating or prosecuting cybercrime cases.

The proposed template of the module for the training of judges is to serve only as the basis for the training of judges and prosecutors and not as the final goal for their training. Project countries/areas should discuss the needs at the national level and request additional specific training in the areas of cybercrime that they identify as most critical.

The lessons that have been prepared provide the headlines/topics of presentations/lectures as well as detailed explanations to be made by the trainers. The course is designed to be amended to meet national requirements, while ensuring that the course aim and objectives are met. This will provide consistency of training modules across borders. Trainers should consider introducing a number of exercises/discussions which will facilitate the learning experience of the participants in each country.

The Basic Training Module is built in such a way that would enable judges and prosecutors that have passed through this module to have basic knowledge of the nature of cybercrime, the terms and the technology. In addition this module provides basic information about international cooperation, electronic evidence, procedural law and investigative measures etc.

There will be an advanced training module that will be an extension and build up of the Basic Module and will provide more detailed information and knowledge about the topics and will use case studies to reinforce the learning in the sessions that are presented in the basic module. The advanced module will be created with the goal of providing the judges and prosecutors with the advanced knowledge that can be applied in practice on the functioning of computers and networks, what is cybercrime, cybercrime legislation, jurisdiction, investigative means and electronic evidence, and international cooperation.

3 How to use the trainers guide

This guide is intended to provide trainers with information on the course structure and content. The objectives for each lesson outline what information should be covered. The training methodology for this course has been prepared and all the relevant training aids should be with this training pack. The aim of this guide is to keep the course standard and ensure consistency during delivery.

This guide is designed to provide some guidance as to the type and level of technology knowledge that is required by judges and prosecutors to fulfil their role effectively. It does not purport to be a complete analysis of the issues and where relevant indicates where further information may be obtained.

It is recommended that training developers ensure that the material they prepare is as up to date and incorporates the latest technology issues as they impact on criminal behaviour; its impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered. There are technological changes that will affect the criminal justice system, such as solid state storage of data and Web 2.0. These will be important issues to include in training programmes and require inclusion as they become more prevalent.

As with any other programme, any training course developed for judges and prosecutors should have clear objectives, which should be SMART (Specific, Measurable, Achievable, Relevant and Time Bound) objectives. This is essential to be able to ensure the objectives are met. Avoid use of objectives with words such as "understand" or "know" as these do not meet the criteria. For example how do you measure if the objective of "knowing" a subject is achieved? It is better to use words such as list or identify, which are measurable.

The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching.

The key role of the training developer is to ensure the overall aim of any learning event and the specific objectives are achieved. This chapter provides some information to assist that process.

Although this course has been developed as a generic, not country specific programme, it is important that trainers personalise their training materials to ensure a more effective delivery of the course material. The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching. Use of physical examples of technology referred to and use of the Internet may also enhance learning. Specifically, the sessions on substantive and procedural law in domestic legislation have been prepared as exemplars of the type of information that should be incorporated at the national level. Trainers are responsible for ensuring that their national legislation is included in these sessions before delivery in country.

4 Course Overview

4.1 How long is the course and who is it for

This course is designed as a 3-day programme for judges and prosecutors as part of their initial training programme.

4.2 Who will deliver the course

The course has been developed in order to be delivered by in house trainers within the judicial training centres of countries. Where necessary, it is advisable that subject specialists are introduced to deal with specific technical subjects if the expertise is not available with the judicial centres. As this is the basic level, it is expected that this course will be delivered to all new judges and prosecutors.

4.3 How will the course be delivered

The course as currently structured is designed to be delivered in classroom setting using classroom based trainer instruction. There is no reason why the materials could not be converted into distance learning or e-learning modules if required. As detailed above, in Section 1, trainers should consider incorporating exercises and other teaching methods in to the programme at the national level.

4.4 Course objectives

The course objectives have been written in a traditional manner that will allow trainers to use various teaching methods to achieve them. All objectives are SMART in order to support this. For those unfamiliar with SMART objectives, the following explanation of the mnemonic is given:

- **Specific -** Objectives should specify what they want to achieve.
- **Measurable** - You should be able to measure whether you are meeting the objectives or not.
- **Achievable** - Are the objectives you set, achievable and attainable?
- **Realistic -** Can you realistically achieve the objectives with the resources you have?
- **Time -** When do you want to achieve the set objectives?

Based on this, the following course objectives have been set and these should be read in conjunction with the overall aim of the course.

4.5 Target students and trainers group

4.5.1 Students

This course is designed for delivery to judges and prosecutors during their initial training period.

4.5.2 Experience Prerequisites

No previous subject knowledge is assumed.

4.5.3 Trainers

Trainers for this course should be employed by judicial training centres where this training will be delivered.

4.5.4 Experience Prerequisites

Trainers should have a good level of knowledge of cybercrime issues/ trends and cybercrime legislation in their country of origin. Previous experience as trainers with knowledge of teaching theory and practice is required.

4.6 Resources

4.6.1 Course Resources requirements

For delivery of this course in a training room environment, the following equipment is necessary:

- A Room of suitable size for the anticipated number of students.
- PC/Laptop running Windows 7 and loaded with MS Office Professional
- Projector and display screen
- Internet access (if available)
- Computer hardware examples (if available)
- Video clip "Warriors of the Net"
- Budapest Convention on Cybercrime including explanatory report
- Copy of the EC OISIN funded e-evidence guide
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Stapler, hole punch and scissors
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily.

4.7 Assessment

No assessment of student knowledge was requested or provided as a part of this pilot course. Countries implementing this training at the national level may wish to introduce assessment. In any event trainers should check the knowledge of students during the course, by questioning, quizzes or other methods to ensure that the learning objectives are being achieved.

4.8 Course and lesson objectives

Lesson Number	Lesson Title	Objectives
1.1.1	**Course Introduction**	▪ Identify the trainers and fellow students ▪ Define course structure and content ▪ Complete relevant administrative tasks ▪ Distribute documentation for course ▪ Explain facilities and procedures at the venue including Health and Safety Issues
1.1.2	**Introduction to Cybercrime**	▪ Identify different types of cybercrime and their impacts ▪ List the threats, trends and tools of cybercrime and responses to the phenomenon. ▪ Explain the concepts of cybercrime that are considered types of crime under most legislation and international standards. ▪ Analyse the needs and the advantages of the harmonisation between national legislation and the international

Lesson Number	Lesson Title	Objectives
		instruments, in particular the Convention of Budapest.
1.1.3 **1.2.2** **1.2.5**	**Introduction to Technology**	▪ List the component parts of a computer system ▪ Identify different types of data storage device ▪ Consider the criminal justice implications of exponential data storage capacity ▪ Identify different computer operating systems ▪ Explain the basics of how networks function ▪ Describe the functions of the Internet ▪ Identify at least 5 major Internet applications ▪ Explain how the Internet has developed from its beginning to today. ▪ Differentiate between different Internet applications ▪ Identify how criminals use the various Internet applications
1.2.3	**Cybercrime as criminal offence in domestic legislation**	▪ List the substantive criminal law provisions, and identify some of the key factors used to describe the crimes, based on the Convention of Budapest. ▪ List the substantive criminal law provisions, and identify some of the key factors used to describe the crimes, based on the existing national law. ▪ Analyse the needs and the advantages of the harmonisation between national legislation and the international instruments, in particular the Convention of Budapest. ▪ Identify the relevant substantive law provisions from case study discussions
1.2.4	**Procedural Law / Investigative Measures in Domestic Legislation**	▪ Explain the procedural provisions of the Budapest Convention ▪ Explain the existing procedural provisions under the national law
1.3.3 **1.3.4**	**Gathering electronic evidence; procedural and**	▪ Discuss various types of electronic evidence ▪ Explain the principles of best practice relating to the seizure and handling of electronic evidence

Lesson Number	Lesson Title	Objectives
	investigative measures	▪ Identify the challenges offered by "dead box", "live data" and Internet sources of electronic evidence ▪ Identify the challenges of obtaining evidence from another jurisdiction ▪ Discuss the issues of admissibility of electronic evidence in judicial proceedings, in terms of its authenticity, accuracy, completeness ▪ Explain the procedural provisions of the Budapest Convention
1.3.4	**International Cooperation**	▪ Recognize the global dimension of Internet and the international dimension of cybercrime ▪ Explain the importance of international cooperation and recognise the available instruments for international cooperation in the field of cybercrime ▪ Identify the need of very fast and efficient channels for international cooperation and the available instruments, the ways they are used, the timelines and effectiveness ▪ Describe the efforts from international organisations regarding the implementation of new modalities of international cooperation ▪ Discuss the Budapest Convention on Cybercrime - identify its general principles, the provisional measures and the 24/7 network on mutual legal assistance
1.3.5	**Course Closure**	▪ Provide appropriate feedback on the course and its effectiveness ▪ Complete the COE course evaluation forms ▪ Identify the next level of learning that they need to undertake to improve their knowledge and skills in the subject matter.

Council of Europe
Cybercrime for Judges and Prosecutors
Training Course

Timetable – Module 1

	09:00 - 10:00	10:00 - 11:00	11:00 - 12:00	12:00 - 13:00	13:00 - 14:00	14:00 - 15:00	15:00 - 16:00	16:00 - 17:00
Day 1	**1.1.1 Course Opening and Introductions**		**1.1.2 Introduction to Cybercrime Threats, trends and challenges**		**BREAK**	**1.1.3 Introduction to Technology Part 1**		
Day 2	**1.2.1 Daily Review**	**1.2.2 Introduction to Technology Part 2**		**1.2.3 Cybercrime as a Criminal Offence in Domestic Legislation**	**BREAK**	**1.2.4 Procedural Law and Investigative Measures In Domestic Legislation**		**1.2.5 Introduction to Technology Part 3**
Day 3	**1.3.1 Daily Review**	**1.3.2 Electronic Evidence Practice and Procedure**		**1.3.3 Electronic Evidence Procedural and Investigative Law**	**BREAK**	**1.3.4 International Cooperation**		**1.3.5 Delegate Feedback and Course Closure**

NB - Coffee and other breaks will be taken at appropriate times during each days training

5 Key Contacts

The following persons are the points of contacts for any enquiries about the course and its content:

Alexander Seger
Head of Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law (DG-I)
Council of Europe,
F-67075 Strasbourg Cedex
Tel. +33 3 90 21 4506
Fax +33 3 90 21 56 50
alexander.seger@coe.int

Mustafa Ferati
Programme Officer
Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law (DG-I)
Council of Europe
67075 Strasbourg Cedex, FRANCE
Tel.: +33 (0)3 90 21 45 50
Fax: +33 (0)3 90 21 56 50
Mustafa.Ferati@coe.int

6 Lesson Plans

6.1 Lesson 1.1.1 Course introduction	Duration: 90 Minutes

Resources required:

- PC/Laptop running Windows 7 and loaded with MS Office Professional
- Projector and display screen
- Internet access (if available)
- Computer hardware examples (if available)
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Stapler, hole punch and scissors
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily

Aim: To provide the delegates with information about the need for the training course and its aim and objectives. To ensure that they have sufficient information about the programme of activities and the timetable. Provide information about the health, safety and administrative details of the course. Introduce the delegates to the trainers and other delegates.

Objectives:

By the end of the lesson the students will be able to:

- Identify the trainers and fellow delegates
- Discuss the overall aim of the course
- Explain why this course is necessary
- List the component parts of the timetable and activities of the course
- List the health and safety procedures for the venue

Slides nr.	Content:
Slides 1 to 23	**Introduction** This is the opening session of the course. During this session the delegates will be introduced to the trainers and the other delegates. The course aim and objectives will be explained along with the methods of teaching. The trainer may choose to introduce "ice breakers" to encourage the delegates to become involved in the course and with each other at an early stage.
	PowerPoint (or other type of presentation) A PowerPoint presentation has been prepared for this session. This is a generic presentation and does not take into account national issues that may need to be dealt with when this course is dealt with at the national level. The trainer should ensure that the information in this presentation is relevant for the location of delivery.

Slide 2	Health and safety issues are dealt with in this slide. These will differ depending on the location of delivery. It is the trainer's responsibility to ensure that they have the correct information to impart to delegates.
Slide 3	The background of the course is provided for the delegates, The title of this course is "Introductory Cybercrime and Electronic Evidence Training for Judges and Prosecutors". It has been developed as an output of the European Union/Council of Europe Joint Project on Regional Cooperation on Cybercrime in the IPA region.
Slide 4	The aims of the session are set out below: ▪ Provide delegates with information about the need for the training course and its aim and objectives. ▪ Ensure that they have sufficient information about the programme of activities and the timetable. ▪ Provide information about the health, safety and administrative details of the course. ▪ Introduce the delegates to the trainers and other delegates.
Slide 5	The individual objectives are the things that that the delegate should be able to do at the end of the session. These objectives may be used to test the knowledge the students have obtained and to allow the students to evaluate the training. For this session the students should be able to: ▪ Identify the trainers and fellow delegates ▪ Discuss the overall aim of the course ▪ Explain why this course is necessary ▪ List the component parts of the timetable and activities of the course ▪ List the health and safety procedures for the venue
Slide 6	This training is necessary because judges and prosecutors play an important role in the investigation and adjudication of individuals or groups that have committed crimes. With the increased number of incidence where these crimes have an element of cybercrime or electronic evidence there is an increased need for judges and prosecutors to be properly trained to understand the nature of these crimes and to also be aware of the legislation and the instruments for international cooperation available to handle cases of cybercrimes.
Slide 7	It is important that the overall aim of the course is explained to the delegates at the very beginning. This will enable them to appreciate the overarching reason for them being there. The overall aim of this course is: To provide judges and prosecutors an introductory level of knowledge on cybercrime and electronic evidence. The course will provide legal as well as practical information about the subject matters and concentrate on how these issues impact on the day-to-day work of the delegates.

Slide 8	The course timetable should be explained to the students at this stage. This should include the times of the course, the lunch and other breaks and a brief description of each session. The inclusion or exclusion of any assessment should be dealt with at this stage. If there is an assessment, this should be explained in detail, including the expectations of the students in terms of study.
Slides 9 to 17	The detailed objectives of each session are set out in the slides. These should be explained to the delegates at this stage. The fundamentals of each lesson are included in the explanation.
Slide 20	The introduction of the trainers and students is the next stage. It is important to take this early opportunity to get them to interact with each other and the trainers. The delegates should be asked to pair with someone in the class that they do not already know. They should then be directed to ask their "partner" the to provide answers to these questions: ▪ Their Name and Country ▪ Where they work ▪ What they do ▪ Their experience as a trainer ▪ Something Interesting about them ▪ Answers to the "knowledge questions":
Slide 21	The "knowledge questions" are designed to create interaction and for the trainers to learn more about the knowledge and experience of the delegates in each of the categories of technology and cybercrime. These are listed on the following slide. Delegates should be asked to indicate which number identifies the closest fit to their knowledge in each of the categories. The pairs should ask the same questions of each other. They should then introduce their "new colleague to the rest of the class. The trainer should keep notes of the information that is provided to assist their knowledge of the students.
	Practical Exercises (if applicable) The only practical exercise in this session is the introduction of the students and trainers and the requirements of this are set out in the previous section.
	Knowledge Check There is no knowledge check with this session
Slide 23	**Summary / Recap** The trainer should recap / test knowledge on the following points to ensure that the students have appreciated the learning objectives of the session. Time should be allowed for questions at appropriate times during the session.

6.2 Lesson 1.1.2 Introduction to cybercrime	Duration: 120 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation

Aim:

The purpose of this lesson is to give to the participants a general overview of cybercrime, both in the legal point of view and in the perspective of new realities. It will cover the background scenario in the different countries and legal framework at the international level.

Objectives:

- During the lesson an explanation to what is cybercrime and why to be worried about it will be provided to the delegates. It will refer to threats, trends and tools of cybercrime, as challenges for judges and prosecutors. Besides, the session will describe national and international responses to this phenomenon.
- By the end of the lesson the participants will be able to identify the realities covered under the expression "cybercrime" and to understand the concepts that are considered types of crime under most legislation and according to international standards.
- The session will cover substantive criminal law provisions, after the most recent developments related to cybercrime offences and point out some of the key factors used to describe the crimes, based on the Budapest Convention and on relevant the relevant legal framework at the European Union level.
- Regarding this last point the need and the advantage of the harmonisation between national legislation and the international instruments, in particular the Budapest Convention will be underlined in this session.

Slides nr.	Content:
	Introduction This session has the specific purpose of giving to the participants a general overview of cybercrime, both in the legal point of view and in the perspective of the effective reality. It will cover the background scenario in the different countries and will refer to the legal framework at the international level.

Slide 2	**Agenda** Part One of the presentation will describe the new realities of the information society and will refer to the emerging illegal activities on the networks. Part Two will recover some of the historic approaches to cybercrime, by some international organisations. Part Three will try to arrive to the reality covered by the eventual concept of cybercrime. Part Four will explain what the Budapest Convention on Cybercrime is and will underline the importance of this single binding international instrument in fighting cybercrime. Part Five will refer to some of the more important illegal activities online, nowadays. Part Six will recover the major topics of all the presentation.
Slide 3	**Session Objectives** The purpose of this session is to present, from a general perspective or as an introduction, the matters relating to cybercrime. The concept of cybercrime will be explained, while discussing the reasons to be worried about.We will discuss heresome of the major threats, trends and tools of cybercrime and also some responses to the phenomenon. An overview of what is covered under the expression "cybercrime" will be provided. Furthermore a description of some of the concepts that are considered types of cybercrime under most legislation and according to international standards will be discussed. One of the most important themes to be discussed relates to the substantive criminal law provisions, and some of the key factors used to describe cybercrimes, based on the Budapest Convention and on relevant European Union legal frameworks. It will be also important to underline the need and the advantage of the harmonisation between national legislation and the international instruments, in particular the Budapest Convention.
Slide 4	**Part One - Information society and cybercrime**
Slides 5 to 7	Information society, a social and economic development model, based on the acquisition and diffusion of information by the means of communication networks, pervaded the daily life of citizens, their workplace, their home and many of their leisure activities.

	In this social and economic environment, there are no physical distances between people in different places in the world. With some very well-known exceptions, in this new "open world", potentially, there are no political frontiers (of the States), between Internet surfers. Here, everybody can obtain democratically information and knowledge, no matter where it is stored. This means also competition between all the economic operators. Information is available to everybody, in a free and open way. Internet users feel that there is no sovereignty over the networks.
Slide 8	As the use of the Internet arrives to every place and to every people in the world, crime increases and criminals discover new possible illegal activities. The crimes committed by the means of the networks are the most transnational of all crimes. This nature raises particular difficulties to those who investigate these criminal activities: on the other side of the world, evidence can disappear if it is not preserved immediately and law enforcement agents must respect political borders. Besides, they need to follow legal proceedings and public channels to request international assistance in criminal investigations.
Slide 9	In this context, the international approach is essential. The multinational or international approach is richer than a mere national or even regional approach and global comprehension of the phenomenon gives a wider dimension. International cooperation between law enforcement agencies – within police or between prosecution services - is crucial to achieve results in criminal investigations.
Slide 10	All observers agree that cybercrime is a global phenomenon and the only adequate approach to address the borderless nature of global networks is a common approach, where domestic efforts are complemented by specific forms and channels of international cooperation that can face the issue of cybercrime being facilitated globally, with potential consequences in any part of the world. It is very clear that cybercrime is a global phenomenon with global dimensions. Each illegal activity, typically, has multiple territorial connections: normally, perpetrators are based in a certain country's jurisdiction, but their actions reach computers and victims in many other countries. This is a common characteristic to other modern forms of criminality, but concerning cybercrime and *e-evidence* in general, it is inherent to its nature. Due to the expansion of communication networks, particularly the Internet, it is impossible for any country in the world to act alone against this crime problem.

Slide 11	Modern societies depend on information technologies. States, citizens and economies are currently connected to the Internet. This is a very fertile field for new emerging illegal activities, within the communications networks, using the networks, or against the networks.
Slide 12	Everywhere, cybercrime is identified with phenomena like *hacking*, or the diffusion of *malware* (mainly viruses or worms), or the popular, within the *media*, computer attacks (*DoS* or *DDos*). However, nowadays, even the common citizen is aware of many other criminal activities on the networks, most of them with profit purposes (vg. regular frauds and computer frauds). And also everybody knows about the great possibilities of utilization of the cyber environment, or cyber ecosystem, to commit or facilitate common crimes.
Slide 13	This expression, "*cyber environment"*, even if it still remains not defined, both in law and academic literature, is each day richer and more complex. Technology is increasing the number and type of devices that can communicate on the networks and that are able to transfer data or just to record them.
Slides 15 and 16	**Part Two - International organisations and cybercrime** Many international organisations have been dealing, for many years, with the question of cybercrime and electronic evidence.
Slides 17 to 20	United Nations is one of the *fora* discussing cybercrime. The United Nations General Assembly adopted, since 2000, formal resolutions on *Combating the Criminal Misuse of Information Technologies* (the first one of them was the Resolution adopted by the General Assembly 55/63, on combating the criminal misuse of information technologies, adopted by the 81st plenary meeting, on 4 December 2000). These formal resolutions point out the need to ensure that a Member State adopts domestic regulations, in view of criminalising certain activities and eliminate the so called *safe heavens* for cyber criminals. UN General Assembly Resolution 64/211 (March 2010) on the "creation of a global culture of cybersecurity" contains a voluntary self-assessment tool for national efforts to protect critical information infrastructure. The Resolution recommends, among other things, that States adopt criminal legislation taking into account frameworks such as the Budapest Convention on Cybercrime. Every five years, the UN organises United Nations Congress for Crime Prevention and Criminal Justice. The 2005 Congress in Bangkok and the 2010 Congress in Salvador (Brazil) agreed on the need for technical assistance and capacity building. Proposals to develop new treaties have not found consensus.

Slide 21	OECD - the Organisation for Economic Co-operation and Development, shares with United Nations the concern on cybercrime phenomena. However, it has developed a different approach. Since 1983, OECD studied the existing need for national cybercrime laws and issued recommendations on that. OECD states that from international to national level, the same criminal facts could be qualified within similar criminal frameworks.
Slide 22	The approach of the Sates of the Group of Eight (G8) goes some steps further, choosing more proactive options. G8 created a network of contact points that became a reference in the international cooperation scenario. Essentially, it is a directory of names that can be reached and could facilitate immediate action where needed. G8 was a pioneer, enfacing cybercrime subjects and, besides the Council of Europe, this is the most important work developed at the international level, combating cybercrime, until these days.
Slides 23 and 24	The European Union (EU) also appears to be alert to cybercrime. In 2005 the EU adopted a binding instrument - the Council Framework Decision 2005/222/JHA[2] of 24 February 2005 on attacks against information systems. This Framework Decision imposes to all Member States the criminalisation of some listed offences: illegal access to information systems, illegal system interference, and illegal data interference. The decision also includes rules referring to instigation, aiding and abetting and attempt. Besides, with respect to international cooperation, the Framework Decision states that all European Union Member States shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. The Framework Decision 2005/222/JHA is currently under revision – since January 2011 (a first public draft of the bill was publish on October 2011).
Slide 25	It is also important to consider the work developed by OSCE, the Organization for Security and Cooperation in Europe, on cybercrime. OSCE issues recommendations to the members of the organization. By Decision No. 7/06, OSCE said that participating States should consider becoming parties to the Budapest Convention on Cybercrime. This decision also encouraged participating States to join the 24/7 Computer Crime Network, managed by the G8 States and to nominate an appropriate contact point for the purpose of streamlining international law enforcement cooperation on combating the criminal misuse of cyberspace.

[2]http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf

Slide 26	The Council of Europe has been dealing with the question of cybercrime since the 1980s. Preparatory work and soft-law recommendations then lead to the decision to negotiate a legally binding international treaty: the Budapest Convention on Cybercrime (this treaty will be discuss later). The approach of the Council of Europe consists of a triangle with: 1. Standards such as the Budapest Convention 2. Follow up and "monitoring" of implementation by the Cybercrime Convention Committee (T-CY) 3. Technical cooperation programmes to assist countries in establishing criminal justice capacities.
Slides 28 and 29	**Part Three - What is cybercrime?**
Slide 30	**Technology as a victim** Technology as a target of crime – is traditionally considered to be true "computer crime" and involves such offences as hacking, denial of service attacks and the distribution of viruses.
Slide 31	**Technology as an aid to crime** Technology as an aid to crime – is where computers and other devices are used to assist in the commission of traditional crimes, for example, to produce forged documents, to send death threats or blackmail demands or to create and distribute illegal material such as images of child abuse.
Slide 32	**Technology as a communication tool** Technology as a communications tool – is where criminals use technology to communicate with each other in ways which reduce the chances of detection, for example by the use of encryption technology
Slide 33	**Technology as a storage device** Technology as a storage medium – is the intentional or unintentional storage of information on devices used in any of the other categories and typically involves the data held on computer systems of victims, witnesses or suspects.
Slide 34	**Technology as a witness to crime** Technology as a witness to crime – can be found when evidence contained in IT devices can be used to support evidence to which it is not obviously related, for example to prove or disprove an alibi given by a suspect or a claim made by a witness.

Slide 35	**Technology crime?** This slide may be used by way of a recap to check that the delegates have understood what has been said so far. It is suggested that the trainer start with the heading only and than ask the delegates to identify the types of crime that we may describe when using the word Cybercrime. It would be useful if the trainer has already understood the different types of crime detailed in the Budapest convention in order that they may use these as examples or to answer questions that may arise from the delegates.
Slide 36	Since 1984, when the novelist William Gibson used the word *cyberspace*, in the science fiction novel *Neuromancer*, referring to the Internet and other networks, the number of similar expressions with the same prefix expanded. *Cybercrime* is among them, of course. Almost three decades later, authors did not achieve a consensus on a precise definition of the expression *cybercrime*, despite the increasing literature that purports to be on cybercrime. Nor is there agreement if cybercrime is really a new and distinct field of penal law, or if it is just a set of individual criminal law provisions, that happen to refer to the digital environment.
Slides 37 to 44	However, sociologically speaking, crime on cyber environments is already an important and autonomous reality. There are, all over Europe, specific investigation units at the police level and some special prosecution services, too. International public organizations and private companies have each time more concern by the consequences of the illegal and harmful acts committed by the means of the communication networks or inside those networks. There is no consensus about the expression *cybercrime*, when lawyers want to address this new reality. Some authors refer to *computer crime*, or *informatics crime*. Others prefer *high-tech crime*. All of them pose the risk of either extending the issue too far, or restricting it unduly. Crime involving computers in not necessarily "high tech". Much of the criminal activities on cyberspace uses relatively simple methods, and poses relatively few technological problems in its investigation. However, maybe this is a false question, because everybody agrees, nowadays, that there is a new social/criminal reality, committed inside or by the means of a computer system. Cybercrime is commonly defined in both a narrow and a broader sense: normally, the expression is used, on a restricted way, to describe a criminal activity in which a computer or a network are an essential part of a crime; however cybercrime is also used to include other traditional crimes in which those same computers or networks are used to make the illicit activity possible. According to this perspective, we are talking about cybercrime where the computer is a tool of the criminal activity (vg, *spamming*, criminal copyright

	crimes committed through *peer-to-peer* networks, etc.); cybercrime in the sense that the computer or the network is a target of the crime such as the un-authorized access, malicious code, etc.; cybercrime where the computer or the network is the place of the criminal activity such as telecommunications' fraud; and finally cybercrime that is facilitated through the use of computers or networks (i.e. *Nigerian fraud*, *hacking*, *phishing*, child pornography, identity theft, etc.) - in the first category, the computer is essential to commit the crime; in the last one, it can be committed by other means, but computers made it easier. Not far away from these realities, some *new age* crimes are just new modalities of traditional crimes which have as distinguishing feature the fact that they just can be committed inside the digital environment. In fact, they cannot, by its nature, occur outside this virtual world and they are generated inside it. It is the case, for example, of computer fraud, or the case of the computer forgery. Some other criminal infringements are committed by the means of a computer system that, despite the use of computers as *medium*, cannot be theoretically distinguished from the same type of crime committed by other ways. Even if they are *online* crimes, this feature does not in and of itself transform them into a new type of crime. Dogmatically, nothing distinguishes them from the traditional criminal law offence. As examples, defamation committed by an electronic newspaper, or the threat committed by email, or even money laundering using an online bank. In this context, there is an even more basic category: traditional *offline* rimes that nonetheless generates digital evidence - for example an attacker filming his "happy slapping" attack on his mobile phone and posting the clip on *youtube*. Even though this incident could not even be called *a cybercrime*, it raises the same evidentiary and investigative issues as cybercrime properly so called. But normally, the type of criminality identified as cybercrime is the category of the crimes that can be characterized as being targeted against the computer environment or ecosystem. As classical examples of this type of crimes, can be pointed out the cases of data interference, system interference such as denial of service attacks, or even illegal access. All these infringements are crimes against the computer system themselves, envisaging the confidentiality, the integrity or the availability of computer data or of the computer system. Often, in a "real" crime scenario, several of these categories will be present together. A criminal might, for instance, threaten a company with a denial of service attack against the company website (crime against the computer system) unless they get paid money (a new version of blackmail using computers as tools), and the threat is communicated via email but could of course just as well been send in a traditional letter).

	In real terms, however, there is a wide range of increasing criminal modalities: typical cybercrimes as *phishing* or the use of botnets are increasing, as well as a great and creative collection of cybercrimes with profit purposes. There is also a significant piracy of software and other issues with intellectual property rights. The diffusion of child pornography material is increasing, so is the value of money laundering over Internet. In general, each day there is an increase in the use of cyber facilities by organised crime and illegal organizations, like terrorist organizations.
Slides 46 to 49	**Part Four - Budapest Convention on Cybercrime**
	The Convention on Cybercrime of the Council of Europe (ETS 185), also known as the Budapest Convention, was opened for signature on 23 November 2001 in Budapest and entered into force in July 2004. By April 2013, 39 States had become Parties to the Budapest Convention (European States, Australia, Dominican Republic, Japan and USA), 10 had signed it (European, Canada and South Africa) and another 8 have been invited to accede (Argentina, Chile, Costa Rica, Mexico, Morocco, Panama Philippines and Senegal). Accession requests by additional countries were in process. Many others have also used the Budapest Convention as a guideline for domestic legislation. The treaty is open to accession by any State that is prepared to implement it into domestic law and to engage in cooperation. The Convention requires States to do the following: – To criminalise offences against computer systems (illegal access, illegal interception, data and systems interference etc.) and offences by means of computers (such as fraud, child pornography and IPR offences). Important: the treaty is technology-neutral and covers conduct not technology or techniques (fraud and not phishing, illegal access and not hacking, system interference and not distributed denial of service attacks etc.) – To provide law enforcement with tools to secure electronic evidence (search and seizure, expedited preservation etc.). Important: these measures apply not only to cybercrime but to any crime involving electronic evidence on a computer system. – To engage in efficient international cooperation through a combination of immediate, provisional measures and formal mutual assistance as well as 24/7 points of contact. All these measures – in particular the procedural law tools – are to meet human rights and rule of law requirements. Article 15 (conditions and safeguards) is therefore particularly important.

	Overall, the Budapest Convention allows Governments to meet the positive obligation of protecting individuals against (cyber)crime and at the same time to respect the rights of individuals when taking action against cybercrime. The achievements to date are: – Process of legislative reforms worldwide – Increased criminal justice measures – Increased trust and cooperation between parties – Global outreach, global impact: 56 countries ratified, signed, invited to accede. Cooperation with at least another 50 countries – Catalyst for capacity building – Increased legal certainty and trust by private sector – An essential element of norms of behaviour for cyberspace – Contribution to human rights and the rule of law in cyberspace – Protecting you and your rights
Slide 51	**Part Five - Some illegal activities online** The goal of this part is to describe very briefly some of the criminal activities developed in the networks.
Slide 52	Phishing ("fishing for passwords") is a technique used to attempt to convince someone to send personal information that other people. That information can be used later to theft or fraud. Normally, the perpetrators use email messages to trick the victims, from who they obtain personal information, including passwords or other access credentials. Sometimes, the technique used is to redirect users to a malicious and fake website.
Slide 53	SPAM is a largely expanded problem. It consists in the diffusion of unsolicited email messages sent out in millions. Those who receive these messages cannot avoid that. Sometimes, the messages just have marketing purposes. But they are often vectors for malware to infect computers. Normally, the sender is someone that the victim does not know and to whom did not ask nor authorise to send messages.
Slide 54	The merger of the terms "*malicious*" and "*software*" led "malware", a term that generically refers to software designed with the aim of accessing a computer system without the consent of the owner or user, or with the aim to damage it. The victim can obtain malware without knowledge, through email attachments or images in messages. This software is normally hostile software and it is inserted in the victim's computer without consent and is built to perform hostile functions or activities.

Slide 55	Viruses are a specific example of malware. Typically, a virus is software with the ability to replicate itself from one file to another and lodging in a particular system – a hard disk or other data storage medium. Normally, just spreads when the infected file is copied or executed. Of course, all this is performed without the consent or even knowledge of the victim and with the aim of causing damage in the computer system.
Slide 56	A worm is very similar to a virus. As the virus, a worm is software that has the ability to replicate itself and to install into a particular system and consume its resources. But it is different from a virus because it spreads itself through a network and does not need to attach to any file.
Slide 57	Adware is also malware. It is software that automatically displays or downloads commercial advertising, without the consent and the intervention of the user. Sometimes it is distributed in conjunction with other software – also available via free downloads. Some types of adware are more dangerous, because they monitor the system, such as the sites visited on the Internet and user preferences.
Slide 58	One of the most intrusive forms of malware is spyware, or software installed on a system without user's consent, with the aim of monitoring the use of the system by the user. Spyware collects information about the user of the system. After that monitoring activity, automatically, the software sends this information to third parties – its specific objective is to hide in the computer of the victim and to report information to someone.
Slide 59	Trojans (Trojan horses) is a name inspired in by the famous horse built by Odysseus, the Greek, and offered to the city of Troy in order to open the gates of Troy from within. It is also the name of malicious software that performs undesirable functions to the user, without his knowledge. This kind of malware can cause destruction of data, disabling security software, facilitating remote access to the computer (to allow someone unauthorised access to the computer) or download and install other malware. Like the original famous horse of the Trojan War, this software is designed to secretly open the computer for penetration from outside.
Slide 60	Botnet is also an acronym (*robot networks*) used to give a name to networks of compromised computers (*zombies*), controlled by one person or organization, with the intention of being used for illicit activities. A botnet is built by the infection with malware, sent by the owner of the botnet. All the infected computers are controlled by software that allows automation of operations across the network. The owner of the network controls its activity and may instruct it to remain inactive until it is necessary. A botnet may consist of millions of zombie computers that are instructed to send spam or malware to individuals or to attack infrastructure. Botnets

	serve multiple criminal purposes and are thus also called the "Swiss army knife of cybercrime".
Slide 62	**Part Six - Summary**
Slide 63	What is cybercrime and why worry about it. Threats, trends and tools of cybercrime and responses to the phenomenon. Realities covered under the expression *cybercrime* and concepts that are considered types of crime under most legislation and on international standards. Need and advantage of the harmonisation between national legislation and the international instruments, in particular the Convention of Budapest.
	Practical Exercises (if applicable) No practical exercises are envisaged for this particular session as there is no guarantee that the level of technology and Internet access to deliver such exercises will be available at all venues. Trainers may in the future seek to supplement to learning by adding exercises, where the training is delivered in an environment where the facilities are suitable.
	Knowledge Check No specific knowledge check in addition to that listed above is currently envisaged for this course. No official assessment has been requested

6.3 Lesson 1.1.3, 1.2.2 & 1.2.5 - Technology	Duration: 330 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- Internet access (if available)
- PowerPoint Presentation
- Computer hardware examples (if available)
- Video clip "Warriors of the Net"

Aim: This session provides information about technology that will be encountered by Judges and prosecutors during their work and which is used by criminals to commit crime and law enforcement to detect it. The aim of the session is to enable the audience to gain sufficient knowledge about technology for them to function more effectively in their roles.

Objectives:

By the end of the lesson the students will be able to:

- Explain the different impacts that technology has on crime
- List the component parts of a computer system
- Identify different types of data storage device
- Consider the criminal justice implications of exponential data storage capacity
- Identify different computer operating systems
- Explain the basics of how networks function
- Describe the functions of the Internet
- Identify at least 5 major Internet applications
- Explain how the Internet has developed from its beginning to today.
- Differentiate between different Internet applications
- Identify how criminals use the various Internet applications

Time	Content:
30 minutes	▪ Introduction and opening (Agenda and Session objectives)
60 minutes	▪ Part 1 – How computers work
60 minutes	▪ Part 2 – How the Internet works
60 minutes	▪ Part 3 – Internet Services
60 minutes	▪ Part 4 – Other relevant Internet applications
30 minutes	▪ Part 5 – Internet Crimes
30 minutes	▪ Part 6 – Summary
Slide nr.	**Content:**

	Introduction **Technology for Judges and Prosecutors** This session is intended to provide trainers with a framework for developing training material to be delivered as part of a wider programme. It cannot be comprehensive as technology changes so rapidly that any detailed technical specifications would be out of date almost as soon as the document is published. Ensuring that judges and prosecutors have sufficient understanding of technical issues as they relate to matters before them is essential to the fair running of any judicial system. This session provides an overview of the relevant aspects of technology and its relevance to the criminal justice system. A PowerPoint presentation is provided as a resource for trainers to use if considered appropriate. An additional resource in the form of the video clip Warriors of the Net is provided to give the delegates a good and clear understanding of how networks function. The video is available from www.warriorsofthe.net and is available in the following languages: English, German, French, Hebrew, Dutch, Swedish, Italian, Portuguese, Danish, Norwegian, Hungarian, Czech, Spanish and Ukranian. This session provides information about technology that will be encountered by Judges and prosecutors during their work and which is used by criminals to commit crime and law enforcement to detect it.
	PowerPoint A PowerPoint presentation with trainer notes has been prepared to supplement this lesson plan and to provide the trainer with examples of how they may develop their own materials to meet the objectives of the lesson. It is important to remember that is it the responsibility of the trainer to develop learning materials that are timely and relevant to the audience and not simply rely on material that has been prepared by another trainer.
Slides 2 and 3	**Agenda** The agenda slides list the parts of the session and the trainer should go through these elaborating where necessary on specific aspects that have emphasis for particular groups of students. The trainer should explain how the materials will be delivered and that there will be time for interaction and questions. The trainer should emphasis that this training is designed to be interactive and that delegates will be expected to participate throughout. The trainer should explain whether there is an assessment and what form that would take, including details of any pass mark that is applied. (For this pilot programme, no assessment is included).
Slide 4	**Session Objectives** It is important that the delegates should understand what the objectives of the lesson are. These should be "SMART" objectives and explained in detail to the delegates before the session begins, using the information on the slide.

Slides 5 to 54	**Part One - How Computers Work** By the end of the session participants should be able to: ▪ List the component parts of a computer system ▪ Identify different types of data storage device ▪ Consider the criminal justice implications of exponential data storage capacity ▪ Identify different computer operating systems
Slide 5	In order for Judges and prosecutors to fully understand the impact of technology on crime, it is necessary for them to gain an understanding of the fundamentals of how the technology they are presented with functions. In particular, in cases involving digital forensics in its broadest sense, this knowledge will provide context and enable informed decisions to be made. This session will provide a basic understanding to computers, their components, the storage of data and the impact of large amounts of data being held on individual devices. Once again the trainer should seek to make this session as interactive as possible and use the information provided to encourage participants to start to consider the impacts on their role of technology and the issues around how such large amounts of data can be manages and introduced effectively into the criminal justice system. If possible, the trainer should acquire examples of the hardware that is referred to in this session, in order that they may be shown to and handled by the participants. There are many other computer components that are not dealt with in this session; however the most important for the purpose of the course are included. For the purpose of developing training programmes it is recommended that components not covered here are explained, depending on the knowledge level of individuals. It would be expected that most recipients of training will understand what a keyboard and mouse are for example, but trainers should not overestimate the knowledge of individuals. Items that may be added to the list above may include: printers, scanners, webcams, modems, speakers, computer and video phones and various storage devices and network connections as well as external ports such as Firewire and USB. In particular see http://computer.howstuffworks.com/computer- hardware-channel.htm for more detailed information about computer hardware; including photographs which will substantially increase the ease with which these concepts may be understood. Remember to obtain permission from the owners of the information if it is proposed to be used in training programmes.

Slide 6	The purpose of this slide is to show that even the most technology literate people could not have envisaged the changes that technology would bring. The delegates are not alone in perhaps not understanding the impact that technology has on their role and the quotes on this slide may encourage them to believe that technology in the criminal justice system should not be feared but embraced with all the necessary safeguards in place.
Slide 7	The trainer should provide a brief explanation of the development of computers from them being standalone, through mainframe terminals into the world of networking, as an introduction to beginning the explanation of computer components.
Slide 8	**Computer components** The trainer should explain that a computer consists of many components and it is relevant for judges and prosecutors to understand the names and functions of these components as they will be referred to in statements and evidence. A brief explanation is provided of each component as follows:
Slides 9 and 10	▪ Motherboard - A motherboard is also known as the main board or system board of the computer. The motherboard is the central circuit board of a computer. All other components and peripherals plug into it. The job of the motherboard is to relay information between them all. The motherboard houses the BIOS (Basic Input/Output System), which is the simple software run by a computer when initially turned on. Other components attach directly to it, such as the memory, CPU (Central Processing Unit), graphics card, sound card, hard-drive, disk drives, along with various external ports and peripherals. ▪ Expansion Ports/Slots – these are the slots on the back of the computer where you can connect sound cards, video cards, wireless adapters, etc.

Slides 11 to 13	▪ CMOS and BIOS - CMOS and BIOS are often used interchangeably; you can think of the BIOS as software, and CMOS as the hardware running it. Abbreviated from Complementary Metal Oxide Semiconductor, CMOS is usually pronounced "see-moss". CMOS is the hardware in a computer that performs very low- level functions and very basic computer start routines. The CMOS does things like maintain a computer's clock, and provides the interface to the rest of the computer hardware for the BIOS to do its job. It requires very little power to operate. Abbreviated from Basic Input / Output System, it's usually pronounced "bye-oss". The BIOS is an interface that allows a user to make low-level changes to a computers motherboard, CPU, memory and other devices. The default BIOS settings are usually set just right. One of the most common changes made to the BIOS in a forensic capacity is to change the order in which the computer looks for devices to boot (start) from. Typically a forensic examiner may use software on a Compact Disk (CD) and will change the BIOS so that the computer starts from the CD and not from the hard disk as this would alter data just by accessing and starting from the hard disk.
Slide 14	▪ Power Supply – The Power Supply Unit (PSU) in a computer regulates and delivers the power to the components housed in the case. Standard power supplies turn the incoming 110V or 220V AC (Alternating Current) into various DC (Direct Current) voltages suitable for powering the computer's components. Power supplies have a certain power output specified in Watts, a standard power supply would typically be able to deliver around 350 Watts. The more components there are in a PC the greater the power required from the power supply.
Slide 15	▪ Central Processing Units (CPU's) - CPU stands for the Central Processing Unit of a computer system. People often mistake the case or chassis of a computer as the CPU. However, the CPU is an internal component of the computer. It cannot be seen from the outside of the system. The first CPUs were used in the early 1960s. With the introduction of the integrated circuit in the late 1970s, it became possible for smaller CPUs to be manufactured as well. This helped transform computers from large, bulky devices that took up entire rooms to more manageable desktop and laptop models. No matter what the type of computer, the CPU works by executing a series of stored instructions known as a program. Most CPUs conform to the von Neumann architecture, which says that the CPU must fetch, decode, execute, and write back the data in a fairly rapid succession. For the layman a CPU is nothing but brain of the computer i.e as what computer actually performs is basically done with the help of CPU.
Slide 16	▪ Memory – Computer memory is technically any form of electronic data storage, although it is most commonly used to describe temporary forms of storage that can be accessed rapidly. It would be a very slow process if the CPU had to obtain data from the hard

	disk every time it executed an instruction; so much data is temporarily stored in temporary memory in order that it may be accessed more quickly. This type of memory is known as Random Access Memory (RAM). The CPU will request data from RAM, process it and write it back to RAM. This takes place millions of times per second. Understanding temporary memory is important in the forensic capture of data from computers as this data is not saved if the power from the computer is disconnected, as is a common feature of search and seizure of computer systems. It is now more common for Law Enforcement to attempt to capture data in RAM before disconnecting the power during computer searches. This is commonly known as "Live Data Forensics". This activity is happening more often as the amount of data that may be lost is greater than the size of the largest hard disk of only a few years ago.
Slide 17	▪ Universal Serial Bus (USB) – USB connectors found on most computers allow for simple attachment of a large number of devices to the computer, such as mice, printers, external storage devices and mobile phones. It is currently the most common method of connecting external devices to computers. Historically, other connection methods such as parallel or serial ports were more problematic as there was a limit to the number of devices that could be connected at one time, and the rate of data transfer were much slower than USB. It is possible to connect up to 127 devices to a computer using USB. The ease with which USB devices can be used means that they are prominent in many digital forensic investigations.
Slides 18 to 20	▪ Hard Disk Drives - Most computers have at least one hard disk and many have more. Larger computers such as mainframes will typically have many hard disks. It is now common for other devices such as CCTV and music players to also have hard disks which can hold huge amounts of data. These disks have hard platters on which information is held and data can be easily deleted and rewritten, while the structure of the disk is remembered, making them viable for long periods of time. Data is stored on the surface of a platter in sectors and tracks. Tracks are concentric circles, and sectors are pie-shaped wedges on a track. Data is stored on hard disks as files which are simply a group of "bytes". Programmes are also files and these are also called by the CPU in order to be used.
Slide 21	▪ Solid State Storage - A solid-state drive (SSD), sometimes called a solid-state disk or electronic disk, is a data storage device that uses solid state memory to store persistent data with the intention of providing access in the same manner of a traditional block i/o hard disk drive. SSDs are distinguished from traditional magnetic disks such as hard disk drives (HDDs) or floppy disk, which are electromechanical devices containing spinning disks and movable read/write heads. In contrast, SSDs use microchips that retain data in non-volatile memory chips[1] and contain no moving parts.[1]

	Compared to electromechanical HDDs, SSDs are typically less susceptible to physical shock, are silent, have lower access time and latency, but are more expensive per gigabyte(GB). SSDs use the same interface as hard disk drives, thus easily replacing them in most applications
Slide 22	▪ CD/DVD/Blu-Ray Disks – These disks may hold varying amount of data and are typically used to store music, video or computer files for distribution. A DVD for example is the same size as a CD and holds about 7 times as much data as a CD. A Blu-Ray disk, which may be used to store high definition content in turn currently holds more than 10 times as much as a DVD. In other words they can store more data than was possible on a hard disk only a few years ago. They all store data in a different way than hard disks and the data held on them is not as volatile as that stored on hard disks.
Slide 23	**Data Storage** It is an everyday practice for evidence to be produced in criminal and civil proceedings that emanates from computers or either digital devices such mobile phones. As technology continues to pervade society, it will become the norm for more and more devices to contain digital evidence that may be used in proceedings. We are already seeing domestic devices being examined to extract such evidence. It is therefore vital that Judges and prosecutors have an understanding of the issues that impact on the integrity and admissibility of digital evidence. As a start point, it will be useful for them to appreciate how data is stored and recovered by investigators. Electronic or digital data is stored in many forms, the most prominent and in many ways the easiest to validate is that stored on computer hard drives. Typical approaches to preservation and production of digital evidence rely on examination on devices in a static condition. In other words when a computer is switched off and data is not in a truly volatile state. Digital forensics examiners are well versed in the requirements of international and national guidelines on the handling of such evidence. One such guide titled Seizure of E-Evidence was developed with funding support from the European Commission Oisin programme and may be found at: http://www.e-evidence.info. This guide promotes the general principles by which most law enforcement work. It is important that Judges have a clear understanding of the way in which data is stored as well as how the evidence is adduced that is presented before them. This requires a fundamental understanding of the concepts of digital data, storage, retrieval and the tools and procedures used to bring that evidence into the criminal justice system. There are numerous resources open to training developers to gather information about hard disk storage to use within learning programmes. One such example may be found at: http://www.storagereview.com/hard_disk_drive_reference_guide. This generally deals with non-volatile storage such as magnetic media, optical storage media, flash memory etc.

	It is now more common for evidence to be recovered from volatile sources such as Random Access Memory (RAM) or devices such as mobile phones where data is more volatile. Judges need to understand the differences in the manner in which such data is recovered and any effect on the integrity of evidence. The importance of recovering volatile data is simply that it is generally lost when a device is powered down and the opportunity to recover large amounts of valuable information that may prove to be valuable evidence has gone. The techniques used to recover this information should comply with the general principles for the preservation and recovery of such data. It is also typical for volatile data to be recovered from networked systems that cannot be shut down for a static analysis to be conducted.
Slide 24	Memory and data storage – this slide gives an outline of the terms used to describe data and it size and is an introduction that will be necessary for the participants to understand the later part of the session which deals with different storage devices and their capacities.
Slide 25	**Operating Systems** In order to function, computers and other digital devices require an operating system. An operating system is a software programme that allows the hardware to communicate with software programmes. Without an operating system the computer would not be able to function. There are different types of operating system depending on the type of computer or other digital device. The most common operating systems in use today are commonly known under the following headings: Windows, Unix/Linux and Apple Mac. There are other systems in use particularly for other types of device such as personal digital assistants and mobile telephones. These are often cut down versions of the major systems although it is now more common for bespoke systems to be developed for some smaller devices. Most applications developed for computers are written for specific operating systems although it is now more common for them to be available for more than one platform. It is important that Judges and prosecutors appreciate the importance of operating systems and are familiar with the fact that different operating systems behave in different ways. There are many references that will enable a training developer to include sufficient information about operating systems to meet the objectives set out for this section. Among these resources are: http://en.wikipedia.org/wiki/Operating_systems
Slides 26 to 28	Operating Systems – these slides give an explanation of the purpose of operating systems, identify the most common operating systems in use today and provide statistical information about the prevalence in use of these systems. Trainers should be aware that they have to keep the information up to date, In particular the information on slide 38 should be updated once a year.

Slide 29	**Digital Devices** The session on digital devices is designed to ensure that judges and prosecutors are able to identify different types of devices that potentially contain evidence. This leads into the later discussion about how much data may be held on devices and touching on some of the challenges that the amounts of data bring to the criminal justice system
Slides 30 to 38	The slides that are included in this session are very extensive and trainers should consider how many of these are necessary to achieve the objective. The session does not however deal with the differences between devices such as mobile phones, thumb drives or computers, in terms of the challenges they create for search, seizure and examination of evidence form these devices. Trainers should consider using examples to support the learning objectives. By this stage of the course, delegates will have been introduced to many technical aspects and it is considered that some of the slides will give them a perspective that is not too difficult to understand and brings some interesting examples to their attention. The important points to cover here are different nature of devices upon which data may be stored and the extent of the challenges that these bring to the criminal justice system. Trainers should consider using examples of where unusual devices have formed crucial sources of evidence in criminal cases.
Slide 39	**Some Different Computers** This short section follows on immediately from that above and is an extension of the discussion on digital devices. Once again, the trainer may use as many or as few of the slides that are relevant to get the message across that evidence may be found on a wide array of devices and that not all devices that may be encountered are what they appear to be. An important feature of the session is the ease of access to devices that may hold many hundreds of thousands of pages of documents that may be evidence.
Slides 40 to 45	The important points to cover here are different nature of devices upon which data may be stored and the extent of the challenges that these bring to the criminal justice system. Trainers should consider using examples of where unusual devices have formed crucial sources of evidence in criminal cases.
Slides 46 to 54	**How Much Data Can They Store** This is an important session that translates the technical information that has been given about digital devices, into the reality of how much information they may hold and what this means in terms of the amount of documentation that may be produced. It is the introduction into later discussions that will take place about the integrity and admissibility of digital evidence and its products.

	The photograph depicted is to provide participants with a benchmark from which to understand the amount of data that may be held on different devices. Trainers are encouraged to use other examples that may have ore relevance in their own country. Another important point to put across is the fact that these devices are no longer expensive and huge amounts of data may be held on different devices. Trainers should also emphasise the challenges if judges and prosecutors make decisions that in effect make the effective handling of huge amounts of data or printed materials, almost impossible.
Slides 55 to 81	**Part Two - How the Internet Works** By the end of the session participants should be able to: ▪ Explain how the Internet has developed from its beginning to today. ▪ Describe the functions of the Internet ▪ Differentiate between different Internet applications ▪ Identify at least 5 major Internet applications ▪ Identify how criminals may use the various Internet applications.
Slide 55	This session provides basic information about the history, functioning and services available on the Internet as well as providing information that allows the participants to differentiate and clearly define the components of the Internet and understand how it impacts on the criminal justice system. Trainers should ensure that examples of a practical nature are introduced to add value to the technical data that is included in the presentation.
Slide 56 to 57	The term INTERNET comes from the contraction of the words INTERconnected NETwork. Many criminal activities involve the use of the Internet and this includes particular types of crime such as hacking, distribution of viruses and phishing attacks as well as more traditional crimes such as fraud. In order for Judges to effectively manage such cases that appear before them, it is necessary for them to understand the fundamentals of the Internet and its applications such as the World Wide Web and email. The following provides an introduction to the subject and provides the template for a successful training module.
Slides 58 and 59	**The History of the Internet** The Internet began its life as the ARPANET in the 1960's. The relevance of this information may not be immediately apparent; however, the fact that the Internet was never designed to be secure may explain why it is comparatively easy for criminals to abuse the systems. The first physical links were created in 1969 with 4 nodes being universities. The first email was sent in 1972 and the following year a new communications protocol TCP/IP was created, which now forms the basis upon which Internet communications take place. The development of the Internet as we now know it was low key in the beginning as there were disjointed separate networks, served only by limited gateways between them. This led to the application of packet switching to develop a protocol for internetworking,

	where multiple different networks could be joined together into a super-framework of networks. This enabled further interconnection, which began to occur more quickly across the advanced networks of the western world, and then began to penetrate into the rest of the world. The disparity of growth between advanced nations and the developing world led to a digital divide that still exists today. There followed the commercialisation of the Internet and the introduction of privately run Internet Service Providers in the 1980s. These enabled more popular access, which really developed in the 1990's. The Internet has had a huge impact on commerce as well as culture. There now exists near instant communication by electronic mail (e-mail) social networking sites, text based discussion forums, and the World Wide Web. The Internet continues to grow, driven by commerce, greater amounts of online information and knowledge. The advent of Web 2.0 is upon us.
Slide 60	The trainer should ensure that information is provided to the participants that will enable them to understand the basics of networking and its limitations. They should be able to differentiate between local and wide area networks. These slides provide that basic information. Trainers should consider giving examples and encouraging participants to discuss different types of networks and how the Internet has developed. An explanation of some common relevant networking terms such as Ports and Bandwidth should be provided at this stage. Delegates should be encouraged to consider their own personal experiences; for example through their Internet access at home or at work.
Slide 61	Local Area Network (LAN) – is a computer network covering a small geographic area, like a home, office, or group of buildings e.g. a school. The defining characteristics of LANs, include their much higher data- transfer rates, smaller geographic range, and lack of a need for leased telecom lines. Wide Area Network (WAN) – is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). Or, less formally, a network that uses routers and public communications links. Contrast with personal area networks (PANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively. The largest and most well-known example of a WAN is the INTERNET .
Slide 62	Ports – are an endpoint or "channel" for network communications. Port numbers allow different applications on the same computer to utilize network resources without interfering with each other. Ports are 'virtual' – NOT the socket you plug into!

	Bandwidth – is the amount of information that can be carried through a phone line, cable line, satellite feed, and so on. The greater the bandwidth, the greater the speed of your connection and the more your Internet experience approaches a more instant-download, TV-style experience.
Slide 63	Network Interface Controller (NIC) – is a circuit board or card installed into a computer that allows it to connect to a network. Media Access Control (MAC) address – is a quasi-unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification and which provides a unique value. Network Hub - or concentrator is a device for connecting multiple twisted pair or fibre optic Ethernet devices together, making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model, and the term 'layer 1 switch' is often used interchangeably with hub. The device is thus a form of multi-port repeater. Network hubs are also responsible for forwarding a jam signal to all ports if it detects a collision.
Slide 64	Network Switch - is a computer networking device that connects network segments. In the past, it was faster to use Layer 2 techniques to switch, when only MAC addresses could be looked up in content addressable memory (CAM). With the advent of ternary CAM (TCAM), it was equally fast to look up an IP address or a MAC address. Router - 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. It is located at the gateway to a network. The term 'layer 3 switch' often is used interchangeably with router, but a switch is really a general term without a rigorous technical definition. Server – is a computer or device that provides information or services to other computers on a network. Given the right software, any network connected computer can be configured as a server. In most cases, a dedicated powerful computer designed to be "always available". One computer can run several services – e.g. web server, email server, file server, print server etc. In a business reality it often makes sense to run different services on different machines for reasons of security and to minimise the impact of any failure.
Slides 65 and 66	**Internet Basics** The Internet can be thought of as the infrastructure over which many different applications can be run simultaneously. If any part of the Internet malfunctions or is destroyed, communication can still continue. No-one owns the Internet – no organisation, no corporation, no government. It is largely self regulated. It all uses the same connection technology. Most modern data networks, like the Internet, are described as "connectionless" or "packet switched". Traffic is split into small packets

	which make their own way from sender to receiver. They do not all follow the same route and are joined together again when they reach their destination.
Slides 67 and 68	Trainers should provide clear explanations about the different applications that run across the Internet, giving clear examples of how these are represented. Consideration should be given to demonstrating examples of each of the applications in addition to the overview given on this slide. There are quite a few Internet Protocols of which the most important is the Internet Protocol (IP). Each computer connected to the Internet MUST use it. An IP Address is your Internet 'telephone number' and without an IP Addresses you would not be able to use the Internet. Different applications and services use different protocols to communicate across networks, some are: HTTP – HyperText Transfer Protocol; SMTP – Simple Mail Transfer Protocol; FTP – File Transfer Protocol; NNTP – Network News Transfer Protocol. *These are said to run "over" IP (not instead of).*
Slides 69 and 70	Most people connect to the Internet through an Internet Service Provider (ISP). These are commercial organisations that rent out space. They keep records…but for how long? There are national and international legal data protection or privacy issues that impact on how long data may be retained by ISP's. This of course has an impact on the ability of criminal justice officials to secure evidence from these sources. Connection is normally made by one of the following methods; Dial-up, Broadband (ADSL), ISDN, Cable, Wireless hotspot or Satellite. Information should be provided about how connections are made to the Internet and participants encouraged to discuss their own experiences. It should be explained that ISPs do keep records but data protection legislation restricts how long they can keep hold of them. The role of the ISP should be explained, explaining their legal status and numbers. This is a good opportunity to discuss the importance of relationship with ISP's in relation to accessing data and conducting lawful interception. The simple terminology is that ISP's rent out their access to the Internet to people – whether they are individuals or organisations. Each ISP will keep certain information about their customers. The details and amount of it will depend on the ISP involved, and it will only last for so long – hours or days depending what is needed. It should be possible to get – Name, address & other info used for registration Date registered, and how the person registered Specific e-mail addresses or screen names unique to the user Financial details like credit cards used to sign up to the ISP Possibly some software detail about the user

	Most importantly, detail of the history of the user's on-line activity – dates, times & duration TIMES ARE VITAL (Time zone issues are dealt with later in this session) It should be pointed out that it is possible to use false details to obtain an account. Can an ISP intercept suspect Internet traffic – YES – but depends on special equipment to record usage and monitors what is happening – so need manpower to do – costs? Also, we have to consider the authority needed to do it. In any event it is necessary to contact the ISP very early into an investigation. Network Address Translation – is a technique where the source and/or destination IP address is re-written as it passes through the firewall or router. It is most common to find it used for multiple hosts on a private network to access the Internet on a single IP address. It is recommended that any training course includes an explanation of Network addressing in some detail and in particular including: the fact that with IP version 4, addresses are in 4 groups of 3 digits (32 bit addressing) with each group numbered from 0 to 255, meaning a maximum of 256 choices. Each group called an Octet (28) and some values reserved. An explanation should be provided with details of how IP addresses are derived. This may be better achieved by a visual representation of the Binary numbering from which they are derived. Further explanation should be given of the difference between static and dynamic IP addresses and the effect this may have on investigations. An explanation of the changes in IP Version 6 should be given and the need for the change in version being that the Internet is running out of IP addresses.
Slides 71 and 72	The extent of the use of the Internet on a global basis is an important feature. The two slides provided here, demonstrate firstly, two different methods of presenting information and secondly, the infiltration of different languages into Internet usage and the changes over a fairly short period of time. As with other time relevant information, the trainer will need to ensure that the information is as up to date as possible and sources acknowledged
Slide 73	**The Internet – How it works** This session is designed to allow the delegates to gain an understanding of how data is passed around the Internet. The information is very basic as required for this particular audience.
Slide 74	In the case of IP, packets are of variable size. Any two packets need not take the same route from source to destination. The recipient computer re-assembles the traffic and if any packets are missing, it requests their re-transmission. The advantage is that the network is a shared resource that can by dynamically allocated depending upon needs at that time. The disadvantage is that it becomes hard to guarantee quality of service as there is no

	dedicated connection. This is being addressed and some voice over IP services offer excellent sound quality.
Slides 75 and 76	The two illustrations on these slides are provided to allow the trainer easily to explain how traffic moves around the Internet
Slide 77	An excellent resource for explaining the Internet is a movie called "Warriors of the Net". It is the perfect tool for introducing Internet to novice users. It helps the newcomers visualise how the Net works. The movie is 12 minutes long. It is about an IP packets journey through net past routers, firewalls and transatlantic cables. It is available for free download for non-commercial use from www.warriorsofthe.net and is currently available (Jan 2012) in the following languages: English, German, Spanish, Hebrew, Dutch, Swedish, French, Italian, Portuguese, Danish, Norwegian, Hungarian, and Czech. A further useful resource in order to establish the level in Internet penetration and growth in countries or regions may be found at http://www.internetworldstats.com/ It is recommended that an element of statistical information is provided within training to ensure that delegates are able to assess the impact of the Internet on their own country.
Slide 78	It is important that the delegates gain an understanding of IP Addresses and the limitations of IPv4. This will help when the later discussion takes place about dynamic and static IP Addressing. This simple information leads into the next section on the future of the Internet
Slide 79	Most ISPs have less IP addresses than customers – rely on the fact that not all will be connected at the same time. Use dynamic IP address allocation to recycle addresses. As the same IP address is quite likely to be used by different people on the same day, time and date (and timezone) are critical when doing ISP checks against suspects. ISPs will offer static IP addresses (which are clearly a requirement for a website for example) – but at a higher cost
Slides 80 to 81	The future of the Internet is an ever changing feast, however the advent of IPv6 will bring many changes to the way we live our lives and also to the criminal justice system. The trainer should explain how IPv6 will enable almost every individual device to have its own IP address and this will have impacts on the way that investigations are conducted in the future. Examples of how the Internet is changing and the affect these changes will make to how investigations are conducted and managed should be provided that are relevant to the particular audience. The effects on bandwidth, commerce and wireless are provided as such examples.
Slides 83 to 111	**Part Three - Internet services**
Slide 83	This session goes into more detail about the services that are available on

	the Internet, in particular the World Wide Web and Email.
Slide 84	Before going into detail about the services available on the Internet, it is worth reflecting on how much countries now rely on those services at the national level. Trainers should provide an overview of the critical national infrastructure in their own countries to ensure that delegates understand how important the Internet has become in national infrastructure security issues in a short space of time.
Slide 85	**World Wide Web (WWW)** The World Wide Web (WWW) was effectively born in 1991 when HTML – Hyper Text Markup Language was invented by Sir Tim Berners-Lee. HTML provided the platform to combine words, pictures and sounds on web pages. Web standards are created by World Wide Web Consortium (W3C). The following explanation goes someway to explaining the name. "The W3 world view is of documents referring to each other by links. For its likeness to a spider's construction, this world is called the Web." *(Tim Berners-Lee, Robert Cailliau; WorldWide Web; Sept 1992*
Slides 86 and 87	Access to the WWW is normally achieved through the use of a Browser, which is a software program designed to locate and display web pages. The most common as of January 2012 are: Mozilla Firefox, Google Chrome, Internet Explorer, Safari and Opera. Trainers should ensure that any statistics such as those given here are updated at regular intervals
Slides 88 and 89	Hyper-Text Transfer Protocol (HTTP) is the common language that Web Browsers and Web Servers use to communicate with each other on the Internet. Though WWW browsers support a variety of protocols, e.g., FTP, NNTP, SMTP, etc., HTTP is the most frequently used protocol in combination with Web browsers. HTTP is a simple request/response (RR) protocol over TCP. Many people mistakenly think that the WWW is in fact the Internet and this is probably because the WWW is the application used by most people. It is common for criminals to exploit that use. In developing a training programme, consideration should be given to including examples of criminal activity on the WWW where they are relevant to the jurisdiction where the training is being delivered.
Slide 90	**Domain Names and IP addressing** This section is designed to provide delegates with a basic understanding of IP addresses and what they mean, without going in to great detail about how IP addresses and domain names relate to each other. The technical detail is considered beyond the scope of this course. It is important that the trainer makes this aspect as easy to explain as possible. The presentation material provided seeks to identify how that may be achieved.
Slides 91 to 93	There are three main learning points that have to be delivered in this section:

	1. Firstly an explanation of a Uniform resource locator (URL) and how it is structured; 2. An explanation of static and IP addressing - Static IP addresses are permanently allocated and effectively always on line. Dynamic IP addresses are allocated each time you go on line, however, seconds after logging off, the IP address may be reallocated. It is for this reason that the exact time of internet access is essential. 3. An explanation of the relationship between an IP address and a URL. - Domain names and IP addresses are interchangeable, if you knew the IP address you should be able to enter that on the address line and be connected to the same site. In practice what normally happens is that you enter the user friendly domain name www.open.gov.uk and servers within the internet system translate it for you and send you to the correct site. In Internet Protocol Addresses the domain name is converted in a unique 32 bit number, normally written in a Dotted Quad notation, a series of four 8 bit numbers written in decimal and separated by periods. As above 212.140.189.10, all numbers in this sequence must range between 0 and 255 (actually 256 alternatives). Obviously in the example given the last number should read 010, however, convention allows this to be shortened to 10 only.
Slide 94	**Traces** An important aspect of dealing with cybercrime is understanding what traces may be left by investigators using the Internet to conduct investigations. This is relevant not only to the investigator but also to the prosecutor that may order investigations and to judges form the perspective of the admissibility of evidence. This section should seek to provide the basic knowledge that will allow participants to understand the risks that going online may bring to an investigation.
Slides 95 to 98	The information provided on the presentation slides gives basic information that should be imparted to the delegates, working through the slides to show what information is left behind by anyone, including investigators who visit web sites. This should be linked to the importance of ensuring that investigators protect their identity in these circumstances and identifying that in some jurisdictions, there may be legal conditions to be fulfilled in order for such investigations to take place.
Slides 101 to 104	**Email** Electronic Mail or Email is a method of exchanging digital messages. To the user, It appears that E-mail is passed directly from the sender's machine to the recipient's; however each message typically passes through at least four computers during its lifetime. 1. A Message is composed on user’s own computer, then sent to ISP's outgoing SMTP mail server* (Simple Mail Transfer Protocol or SMTP)

	2. Outgoing ISP forwards e-mail onto recipient's ISP SMTP mail server* (SMTP – SMTP) 3. Recipient's mail server finds recipient's incoming mail server (Post Office Protocol or POP3) and delivers message to 'recipient's post box' 4. Recipient logs onto account and message is retrieved into recipient's inbox, normally deleting it from the mail server in the process * *Mail server – dedicated computer used to handle mail*
Slide 105	There are different types of electronic mail; E-mail - The traditional Outlook type mail – sent via SMTP – retrieved via POP3 and once downloaded resident on your own machine Web-based mail **-** POP3 mail; for instance using Outlook Express – when you log in you normally download all new mail into you inbox resident on your machine; IMAP mail – 'true' web-mail – viewed via your machine but still resident on a remote server – can be organised into folders, etc. but only visible when online.
Slides 106 to 109	**Email headers** It is often easier to compare email to a letter when explaining email. E- mail messages have a header part (the envelope), and a body part (the letter itself) with attachments. The message header is the primary focus for investigators as it contains information about sender, recipient, IP-addresses, mail servers, time-stamps etc. This information is used to assist the tracing of the sender of a message where it is not immediately apparent, for example in the case of a ransom demand issued via email. The full or extended header is vital to tracing the source of a message and it is important that Judges appreciate the difference between the headers seen when a message is delivered and the extended header that contains all the relevant information. Email is one of the most common applications that will be encountered by Judges and training designers should ensure they include the most up to date information on different types of email and how evidence about them is correctly obtained from messages themselves as well as the Internet Service Providers through who services the messages pass. Further information about email works that may be of use to training designers may be found at http://www.learnthenet.com/english/html/20how.htm
Slides 112 to 159	**Part Four - Other Relevant Internet Applications** This section of the course is designed to give the participants an overview of the applications on the Internet that are not included in the previous sections. These are necessary as they will be encountered in the normal course of the activities of the target audience. This information will support the objectives of the course. The level of detail provided is considered suitable for the level of teaching that is required. Care should be taken by the trainers not to provide too much in depth knowledge as this will be included in the advanced course that is being developed.
Slides 113 to 114	**Online Storage** **Cloud Computing**

	Cloud computing is a marketing term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. A parallel to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and typically involves provisioning of dynamically scalable and often virtualised resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programmes were installed locally on their own computers. Cloud computing providers deliver applications via the Internet, which are accessed from web browser and desktop and mobile apps, while the business software and data are stored on a server in a remote location. In some cases, legacy applications are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data centre location; in other cases, entire business applications have been coded using web0based technologies such as AJX. At the foundation of cloud computing is the broader concept of infrastructure convergence and shared services. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance. It enables IT to more rapidly adjust IT resources (such as servers, storage and networking) to meet fluctuating and unpredictable business demand. Most cloud computing infrastructures consist of services delivered through shared data-centres and appearing as a single point of access for consumers computing needs. Commercial offerings may be required to meet service-level agreements but specific terms are less often negotiated by smaller companies. The tremendous impact of cloud computing on business has prompted the federal US government to look at the cloud as a means to reorganise its IT infrastructure and decrease its IT budgets. (Source www.wikipedia.com) Issues relating to the identification and collection of data from the cloud and the legal implications of such actions are dealt with elsewhere in this course.
Slides 115 and 116	Information may be provided by the trainer about the prevalence of online storage and as an example the number of Google searches and the increase over a period of time, gives an idea of the interest that there is in such storage. Information should be provided about the different types of online storage differentiating between free and paid for services. The fact that criminals may use this type of storage should be made clear.
Slide 117 and 118	Different ways in which criminals use the Internet services should be of interest to the participants. One such use is by was of a "dead letter box". This may be explained by the trainer as it is fairly easy to understand how this method of communication may be used with little risk of capture.

Slides 119 and 120	**Peer to Peer (P2P)** Peer to Peer services have for many years allowed the transfer of illegal files as well as files that are subject to intellectual property rights. Peer to peer clients have been popular among criminal groups involved in these activities. First generation peer-to-peer architecture worked on the principle of using a centralised server to which people connected in order to download files. This made identification of those offering illegal services fairly easy to locate and close down. Second generation peer to peer clients use different methods of connectivity from those that hold lists of available files to make searching easier to those that act as supernodes that identify where files are available. Judges will need to be aware of peer to peer activity as it may be relevant to many types of criminal and civil trial. An in depth knowledge is not necessary and training designers should consider using sites such as http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126 to provide up to date information.
Slides 121 and 122	**Newsgroups** The term Newsgroup is somewhat of a misleading description as they tend to host discussions. They are technically different but function in a similar way to discussion forums hosted on the World Wide Web. Newsgroup servers are hosted by various organisations who agree with others that they will synchronise their information on a regular basis. This allows users to post messages to one server and be seen by a larger audience.
Slides 123 and 124	**File Transfer Protocol (FTP)** FTP is a powerful protocol that allows the transfer of files from one computer to another. It works on a client/server basis with an FTP programme installed on the client allowing the user to interact with a server in order to gain access to the services and information on the server. When a user wishes to transfer a file a TCP connection is create to the target system. User ID and password are allowed to be transmitted and the user is allowed to specify the files and the action required. When approval is given for the file transfer, another TCP connection is created for data to be transferred. Why do Judges need to know of the existence of FTP services? The answer is that they may encounter the use of such files in cases where criminals are exchanging files with each other or where FTP is used as the method of transfer by other protocols such as Internet relay Chat (IRC).
Slides 125 and 126	**Internet Relay Chat (IRC)** Internet Relay Chat (IRC) is in effect a teleconferencing system that is somewhat dated but still used by criminals to communicate and exchange files. It works by a series of servers connecting to each other and sharing messages that are posted in "Channels", which are text based, virtual meeting rooms. The discussion topics are listed and users who have an IRC client may connect to one or more channels at any time to engage in discussion with likeminded people. IRC is not the most user friendly service on the Internet and is mostly used by those who are more experienced and potentially older users. It is a protocol used by criminals and a rudimentary knowledge of its functions is required by Judges and prosecutors.

Slides 127 to 132	**Instant Messaging (IM) and Social Networking** Instant Messaging and Social Networking have taken over as the communications tool of choice in recent years with many well known examples providing instant and user friendly access to other users throughout the world. The main feature of these sites is the ability to create a personal profile and share information about yourself and to meet new people. It is possible to share photos music and videos. The amount of personal information that is posted by individuals can make them a target for criminals for example those involved in identity theft and those wishing to groom children. Further information that may assist in the development of training materials may be found at http://communication.howstuffworks.com/how-social-networks- work.htm . Instant messaging is a form of real time direct chat between two or more individuals using shared clients. This type of chat involves contact between known person as opposed to other types of chat that allow communication between unknown persons. Criminals are known to use instant messaging as a method of communication. Further information may be provided by the trainer in the form of statistical data about the increase in the use of social networking. Examples of the growth of specific sites and the global impact are provided as examples. The trainer should consider providing examples of the types of information that is available to investigators. Some examples are provided in the presentation that may be of use, although trainers should try to find examples relevant to the geographical location of the participants.
Slides 133 to 136	**Online Gaming** An online game is a game played over some form of computer network. This almost always means the Internet or equivalent technology, but games have always used what technology was current; modems before the Internet and hard wired terminals before modems. The expansion of online gaming has reflected the overall expansion of computer networks from small local networks to the Internet and the growth of Internet access itself. Online games can range from simple text based games to games incorporating complex graphics and virtual worlds populated by many players simultaneously. Many online games have associated online communities, making online games a from of social activity beyond single player games. The trainer should seek to provide examples of crimes involving gaming. These are becoming more prevalent and it would be useful to consider the legal implications in various countries.
Slides 137 to 146	**Internet Anonymity and Traceability** Internet anonymity is an important subject to be covered at the basic level on this course. These terms will be encountered by judges and prosecutors

	on a regular basis. Examples of anonymous services should be given with an explanation of how they work. The difference between anonymous and transparent transmission should be explained. The slides provided in the presentation may assist trainers in developing their own materials. The trainer should provide examples for both web and email anonymity services.
Slides 147 to 159	**Part Five - Internet Crimes** As the final substantive section of the lesson, the trainer should seek to identify ways in which the technology that has been explained is used in the commission of criminal offences. Really the only country in the world that collates Internet Crime complaints is the United States. The statistics provided by the Internet Crime Complaint Center at least provides some impression of the scale of problem. These may be used and should be kept up to date by the trainer.
	Investment schemes Using the Internet to solicit financial support for high tech schemes such as virtual shopping sites or new service providers ***Credit-card schemes*** Using unlawfully obtained credit card details to purchase high value goods over the Internet ***Business Opportunities / Work at Home Schemes*** Internet used to advertise business opportunities whereby victim pay up front for information ***419 Frauds*** West African frauds – means of delivery has changed – it's now electronic mail instead of traditional mail or fax requests otherwise nothing changes – potentially vast access by spamming. ***Internet Banking*** Simply copy a banks web-site, change the web-address slightly, provide links to legitimate bank services and just one or two links to high yield investments that require transfers of significant sums to ensure inclusion in a truly unbelievable investment opportunity. ***Disaster Charity Appeals*** Within 1 hour of Far East Tsunami, web-sites appealing for aid to the victims had arrived on the Web, many (if not all at this time) were bogus ***Herbal Viagra*** In the area of alternative medical treatments on-line, spammed to 'customers', most of the products have no beneficial effects (if delivered at all), some are just outright dangerous ***Russian Brides*** Sites offering contacts with beautiful East European females and cheap visits to Russian states

	Lottery Wins Request for payment to claim lottery winnings or assistance to win (often foreign lotteries) ***Phishing*** E-mail messages pretending to be from well-known source (such as bank, or an internet service provider) asking to confirm personal information. The trainer should seek to identify relevant cases from the region in which the course is being held and use these as examples. At the end of the session, the trainer should encourage the participants to share their own knowledge and experience of internet crimes.
	Practical Exercises (if applicable) No practical exercises are envisaged for this particular session as there is no guarantee that the level of technology and Internet access to deliver such exercises will be available at all venues. Trainers may in the future seek to supplement to learning by adding exercises, where the training is delivered in an environment where the facilities are suitable.
	Knowledge Check No specific knowledge check in addition to that listed above is currently envisaged for this course. No official assessment has been requested
Slides 160 to 162	**Part Six - Summary / Recap**
	The trainer should recap / test knowledge on the following points to ensure that the objectives for the participants as listed have been achieved: ▪ Explain the different impacts that technology has on crime ▪ List the component parts of a computer system ▪ Explain how data is stored on computer systems ▪ Identify different computer operating systems ▪ Explain the basics of how networks function ▪ Describe the functions of the Internet ▪ Identify at least 5 major Internet applications ▪ Explain how the Internet has developed from its beginning to today. ▪ Differentiate between different Internet applications ▪ Identify how criminals use the various Internet applications This may be achieved by way of group discussion, questioning of the participants, a quiz or other recognised methods. This lesson has sought to provide some guidance as to the type and level of technology knowledge that is required by Judges and prosecutors to fulfil

	their role effectively. It does not purport to be a complete analysis of the issues and where relevant indicates where further information may be obtained. It is recommended that training developers ensure that the material they prepare is as up to date and incorporates the latest technology issues as they impact on criminal behaviour; its impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered. There are technological changes that will affect the criminal justice system, such as solid state storage of data and Web 2.0. These will be important issues to include in training programmes and require inclusion as they become more prevalent. As with any other programme, any training course developed for Judges should have clear objectives, which are SMART (Specific, Measurable, Achievable, Relevant and Time Bound). This is essential to be able to ensure the objectives are met. Avoid use of objectives with words such as "understand" or "know" as these do not meet the criteria. For example how do you measure if the objective of "knowing" a subject is achieved? It is better to use words such as list or identify, which are measurable. A guide to setting SMART objectives may be found at www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching. The key role of the training developer is to ensure the overall aim of any learning event and the specific objectives are achieved. This chapter provides some information to assist that process.

Potential Additional Resources

The following is a list of publications from organisations/countries that may be of use to the trainers in developing course materials in relation to electronic evidence.

Organisation	**Country of origin**	**Example documentation**
International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)	International	ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories (18.10 Electronic evidence class, 01 Data preservation, .02 Data analysis) ISO/IEC CD 27037 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence ISO/IEC 9797-2:2011 Information technology -- Security techniques --

		Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
European Network of Forensic Science Institutes (ENFSI)	EC	EA-5/03 Guidance for the implementation of ISO/IEC 17020 in the field of crime scene investigation
Association of Chief Police Officers (ACPO) PCeU Police Forces of Wales E-Crime Wales	England, Wales and Northern Ireland Wales	Good Practice Guide for Computer-based Electronic Evidence. First responder guide: an investigators' 1st responder guide for the initial response to computer related incidents.
ACPO	England, Wales and Northern Ireland	Advice and Good Practice Guide: For Managers of Hi-tech/Computer Crime Units.
ACPO	England, Wales and Northern Ireland	Managers' Guide: Good Practice and Advice Guide for Managers of e-Crime Investigations.
British Standards Institution (BSI)	UK	ASTM E1732 – 11 Standard Terminology Relating to Forensic Science ASTM E1492 – 11 Standard Practice for Receiving, Documenting, Storing, and Retrieving Evidence in a Forensic Science Laboratory
United Kingdom Accreditation Service (UKAS)	UK	Publications relating to Certification Body accreditation
Forensic Science Regulator (FSR)	UK (Home Office)	Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System Minutes of the Digital Forensics Group
The Institution of Engineering and Technology (IET)	International (the IET incorporates the IEE (Institution of Electrical Engineers) and the IIE (The Institution of Incorporated Engineers)).	Development of standards in emerging and established technology fields.
European Cybercrime Education and Training Group (ECTEG)	EC (Europol)	Minutes of ECTEG meetings

British Computer Society, Cybercrime Forensics Specialist Group	UK	Policy documents
US Department of Justice	US	Forensic Examination of Digital Evidence: A Guide For Law Enforcement
FBI/SWGDE	US	Digital Evidence: Standards and Principles
US Dept of Commerce	US	Guidelines on Cellphone Forensics
International Organisation of Computer Evidence	International	Guidelines on Digital Evidence
Council of Europe	EC	Cybercrime Convention legislative and procedural requirements for countries wishing to ratify the convention
Interpol	International	Cybercrime Manual
Skills for Justice	UK	National occupational standards for countering e-crime, provide knowledge and skills standards for handling of digital evidence, digital forensics and cybercrime investigations.
US Secret Service (US Department of Homeland Security)	US	Best Practices For Seizing Electronic Evidence v.3A Pocket Guide for First Responders
European Commission	EC	Seizure of "e-evidence" Oisin Project 2002/OIS/014
National Institute of Justice (NIJ) (National Institute of Standards in Technology NIST)	US	Electronic Crime Scene Investigation A guide for first responders (2nd Edition)

6.4 Lesson 1.3.1 - Daily Review	Duration: 30 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation

Aim:

The purpose of this session is to review the previous days activities, obtain feedback from the delegates and check that the objectives of the sessions have been met

Objectives:

By the end of the lesson the students will be able to:

- Identify areas of the previous days activities that they have understood
- Identify such areas where they need to review the materials to bring their knowledge to the required level

Introduction

This session has been prepared to allow students to check that they have understood the previous days teaching and that they are able to meet each of the objectives for the individual sessions. It is also to provide the trainer the opportunity to check the knowledge level of the students and to identify areas where the teaching materials may be improved.

Slides nr.	Content:
Slides 1 to 12	**PowerPoint** (or other type of presentation) The slides in this presentation are provided to assist the trainer and the delegates with the previous days' activities. The trainer should recap on those activities using the agendas and objectives as the benchmark.
	Practical Exercises (if applicable) No practical exercises are prepared for this session
	Knowledge Check The trainer should check knowledge by asking relevant questions from each of the session aspects.
	Summary / Recap This whole session is designed as a recap of the previous days activities and no separate recap is required

6.5 Lesson 1.2.3 Cybercrime as criminal offence - Domestic legislation	Duration: 90 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation

Aim:

The purpose of this session is introducing the participants to national regulations on cybercrime, the types of criminal infringements described and relevant and applicable international legal framework.

Objectives:

By the end of the lesson the students will be able to:

- Identify national regulations on cybercrime
- Identify the types of criminal infringements described under national law
- Identify some specificities of the national regulations on cybercrime, in the context of the international legal framework scenario

Introduction

The objective of this session is to provide all the necessary information and background to judges and prosecutors to enable them to effectively use the legal provisions in the local legislation to prosecute and adjudicate cases of cybercrime. By the end of the session the participants will be able to identify the legal provisions in the domestic legislation pertaining to:

- Offences against the confidentiality, integrity and availability of computer systems and data
- Offences by means of computer data and systems
- Content related offences etc

This session has been prepared to provide students with an example of how the Budapest convention has been incorporated into the national legislation of one country, in this case Portugal. Trainers will need to replace the Portuguese information with the corresponding legislative details from their own country.

Slides nr.	Content:
Slides 1 to 66	**PowerPoint** (or other type of presentation) The content of the slides in this section are only an example of what can be described in each of the local trainings. Ideally, the session on substantive national law should mention the international legal instruments signed or ratified and the result of its transposition to the domestic law. Besides, a descriptionof the types of crimes according to national lawand, at the end, if applicable, a description of any eventual specificities of the national substantive law should be provided

Slide 2	**Agenda** This session has four parts: 1. Part One, will focus on the Substantive Criminal Law of the Budapest Convention on Cybercrime. 2. National Substantive Criminal Law, will be the object of Part Two. 3. Part Three will focus on Case Studies. 4. Finally, a summary of all parts will be presented in Part Four.
Slide 3	The trainer would cover the following points: ▪ The substantive criminal law provisions and some of the key factors used to describe the crimes, based on the Budapest Convention ▪ The substantive criminal law provisions and some of the key factors used to describe the crimes, based on the existing national law. ▪ The needs and the advantages of the harmonisation between national legislation and the international instruments, in particular the Budapest Convention.
Slide 4	▪ The relevant substantive law provisions based on the discussions relating to the presented case studies
Slides 5 and 6	**Part One - Budapest Convention on Cybercrime – Substantive Criminal Law** As the first international treaty on cybercrime, the Budapest Convention aims to facilitate and develop international cooperation in criminal investigations. A primary goal is to harmonise substantive law between the Parties to permit cooperation. For this purpose, Budapest Convention defines ▪ Offences against the confidentiality, integrity and availability of computer systems and data. ▪ Offences by means of computers.
Slide 7	This section refers to one of the most important categories of cybercrime: offences against the confidentiality, integrity and availability of computer data and systems. This may called cybercrime in the narrow sense.
Slides 8 and 9	The crime of illegal access is committed by those who access the whole or any part of a computer system without right. This action must be intentional and it is described under Article 2 of the Convention of Budapest. It is very often referred to as *hacking* of computer systems and is one of the most common computer crimes. However, there are other phenomena, besides *hacking*, that can be classified as illegal access – in fact *hacking* is used, normally, to describe the act of unlawfully accessing a computer system, by the means of technology. But illegal access also covers any non-authorized entering in a system, regardless of the technology used or even the use or not of technology. Such case, for example, would be the unlawfully

	obtained password by the perpetrator. The protected interest here is the confidentiality of a computer system and data.
Slides 10 and 11	Illegal interception, described under Article 3 of the Convention of Budapest, is also an intentional infringement. It is committed by those that, without right, intercept non-public transmissions of computer data, to, from or within a computer system, by technical means. This provision protects the integrity of non-public transmissions of computer data, criminalising their unauthorised interception. Data transmissions to a computer system, or from that system, or within the same system, are most relevant realities in nowadays life on the networks. Technically, it can be very easy to intercept communications if the network and the communication are not properly protected. An interception of communications can reveal, for example, which websites someone visited, or the email messages he or she sent or received. The crime of illegal interception aims, therefore, to enface the vulnerability of the communications technology, protecting the secrecy of non-public communications.
Slides 12 and 13	Those who, intentionally and without right, cause damaging, deletion, deterioration, alteration or suppression of computer data, will commit the crime of data interference, described under Article 4 of the Convention of Budapest. Data interference protects the integrity of data against unauthorised interference. The owner of the data has the right to keep them as they are, as the owner of a good, in the real life, has the right to keep his property safe from interference from others. In some jurisdictions, regular and classic damage also covers data interference; in others, there is a need to describe separately the damage on computer data, or data interference. This crime enfaces the great increase of relevant data (computer data) to the modern life. Computer data are very vulnerable and can very easily be destroyed or manipulated. This criminal rule protects its integrity and its availability. One of the most frequent cases of data interference is the result of the action of viruses – that without right install themselves on the computer of the victim and, for example, delete data.
Slides 14 and 15	System interference is the hindering of the functioning of a computer system – the serious hindering: Article 5 of Budapest Convention does not cover non-serious hindering. This effect can be the result of inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, if this is committed intentionally and without right. This particular aspect excludes, in general, for example, security tests, conducted by the administrator of the network. This infringement covers a wide range of acts,

	able to interfere with the normal and proper functioning of a network. In fact, Budapest Convention recognises the importance of the communication systems and of the computer technology in the everyday life – the availability of these systems is crucial for the regular functioning of public, economic and social activities. But this type of crime does not only cover interferences on a big scale, like denial-of-service attacks. Even small actions, just envisaging one computer, can be system interference – it will be the case of *mail bombing* targeted to a single email address. In fact, it will have always a crime of system interference when a perpetrator targets a computer system with more requests than that system can manage. This crime envisages protect the access to communication networks, both protecting the operators of the system and the end user.
Slides 16 to 19	One of the most complexes infringements described on Budapest Convention is the crime of misuse of devices – Article 6. Like with other crimes, the action of the perpetrator must be intentional and without right. Covers a wide range of activities, all of them related with devices which are able to be misused. This is a very "new" crime, not included in the Recommendation of 1989. It is also very innovative - the facts described in there were not recognised previously as a crime in many of the national legislations. Essentially, it prohibits the production, sale, procurement for use, import, distribution or otherwise making available of devices, including a computer program that are designed or adapted primarily for the purpose of committing any of the other substantial offences named in the Convention. Equally, it criminalises the sale of computer passwords, access code, or similar data by which the whole or any part of a computer system is capable of being accessed. With this provision, the Convention recognizes the need of incriminating the flourishing and increasingly economically important "secondary market" in "crime enabling equipment": hackers selling online their tools of the trade, self-made virus kits widely available online and wholesale disposal of passwords that were stolen using Trojans and other devices. This means that *hacking* into a computer system is not any longer the preserve of highly skilled programmers. Every "regular" criminal can easily buy the necessary tools, or directly the stolen passwords - very often the criminal seller will offer also a "customer service" and help his client setting up his computer for the commission of a crime. One of the most discussed details of Article 6 refers to 1, b, that (still intentionally and without right), incriminates the possession of *a device* with the intent that it is used for the purpose of committing any of the offences established in Articles 2 to 5 of the Convention (illegal access, illegal interception, data interference and system interference). This option is similar to what some jurisdiction call "preparatory acts" that, in

	this case, are already and autonomously criminalised.
Slide 20	Computer-related offences are crimes committed by the means of a computer system. These infringements are new modalities of traditional crimes, but they just can be committed within the digital environment and they cannot happen outside this virtual world.
Slide 21	Computer-related forgery, described under Article 7 of Budapest Convention is a particular modality of forgery. In most countries forgery is a traditional criminal infringement. But normally, it refers to tangible objects and sometimes cannot be used to criminalise computer forgery, or forgery of computer data. That was the reason of introduction in the Convention of Article 7. At this point, the Convention aims to introduce a parallel offence to the traditional forgery of documents (tangible documents). But in this case, the object of the crime is computer data. This crime is committed by those who input, alter, delete or suppress computer data, resulting in inauthentic data with the intent that those data are considered or acted upon for legal purposes as if it were authentic. This crime requires, of course, and intentional and without right action.
Slide 22	Computer-related fraud, described under Article 8 of Budapest Convention, is a type of crime that just can, dogmatically speaking, be hardly distinguished from the traditional fraud, as a criminal offence. However, it is, in fact, a new and autonomous modality of that traditional crime. Just can be committed inside the digital environment. Most domestic laws criminalise traditional fraud, but it is, normally, unusable to computer related situations. Fraud requires a falsity, or an intentional mistake caused by a person. But most of the times, in computer fraud, there is not a direct intervention of a person and is just the result of the manipulation of a computer system. That is the reason why in the description of the type of crime of computer fraud, the intervention of a person, as a perpetrator, is replaced by the undue manipulation of data, with the intention of obtaining, without right, an economic benefit. In this way, it is not necessary to have the deception of the mind of another person as an element of fraud.
Slide 23	Content-related offences refer to those crimes that became easier through the use of computers or networks. These kinds of infringements can be committed by other means, but computers and networks made them easier.
Slides 24 to 26	Article 9 of Budapest Convention discloses one of the great innovations of this treaty: it criminalizes child pornography acts committed by the means of a computer system. The trade with child pornography increased enormously with the advent of Internet. The communication and information networks offer a great number

	of advantages and possibilities for those who look for such kind of content. Besides, on Internet, the users can be anonymous, while gaining access to child abuse material online. Concerning child pornography offences, one aspect in particular must be discussed, because it is broadly considered in the text of the Convention: the punishment of the mere possession of child pornography materials. Article 9, 1 defines as an infringement the mere possession of this kind of material, within a computer system and also the procurement of such images for purely personal use. This approach is commonly adopted by other international *fora* that studied the theme. Equally contentious is the criminalisation of "pseudo images". The articles of the Convention cover not only situations of pictures where a real child is photographed during sexual activity, but also fake representations of children – for example, pictures of children completely created by computers (morphing for instance the head of a child on the body of the adult that commits the sexual act) or pictures from adults (convincingly) pretending (acting or dressing like) to be children. Criminalising the mere possession of child pornography material is making it much easier to conduct a criminal investigation into this topic, since under this provision anyone who has in his possession this type of material can be prosecuted, and the specific intent to use the pictures in a certain way (for example sell them) or participating in their production does not need to be proven. This also means that suspected paedophiles can be punished without any evidence that they acted on their impulses towards a child. And of course, police and courts can investigate and convict this way suspected suppliers of child pornography (even if by the mere possession), with or without evidence that actual trade took place. At In this respect, it is important to also consider the legal option from the European Union. For many years, the European Union decided to criminalise the mere possession of child pornography materials - since the Decision from the Council from 29 of May of 2000. More recently, Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011, on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, stated that Member States from the European Union should criminalise, among other illegal behaviours, the acquisition or possession of child pornography (Article 5, 2). However, the same document gives discretion to each of the Member States to decide whether this incrimination applies to cases where that pornographic material possessed by the producer solely for his or her private use (in so far as no pornographic material has been used for the purpose of its production and provided that the act involves no risk of dissemination of the material). This option from the European Union is absolutely in line with Article 9 of Budapest Convention that incriminates producing, offering or making available, distributing or transmitting, procuring or merely possessing child

	pornography in a computer system or on a computer-data storage medium. However, the inclusion of "procuring" or "possessing" allows reservation from the Parties to the Convention. This option was reinforced by the Convention on the Protection of Children (CETS 201), issued by the Council of Europe and opened for signature in 2007. The aim of this treaty is to harmonise criminal law provisions, within the Parties, aiming to protect children from sexual exploitation. According to Article 20, among others "*procuring child pornography for oneself or for another person*" and "*possessing child pornography*" should be criminalised
Slides 27 and 28	Budapest Convention does not include any provision with specific offense on copyright matters. However, Article 10 of the Convention refers to it, even if does not create conceptually new regulations on this subject. Rather, the Convention only emphasises that previous rules on copyright in the real world should apply to the online environment: what is prohibited in the real life must also be prohibited online. Infringements of copyright online, or committed by the means of a computer system, must be punished as if they were committed in the real world. For this reason the Convention refers to already existing international treaties and agreements on this matter (Paris Agreement from 24 of July of 1971, Bern Convention and WIPO treaties).
Slide 29	Two final issues, referring to substantive penal law, must be considered at this point: the punishment of aiding and abetting, on one hand, and the criminal responsibility of legal entities. Article 11 of Budapest Convention describes acts of aiding and abetting that all the Parties of the Convention must consider in their domestic law. However, it recognises that internet crime is often a "multi-party" activity with often unclear degrees of contribution by different parties, making prosecution potentially difficult.
Slide 30	Finally Article 12 of the Convention requires from all the Parties the criminalisation of acts of legal entities. This is an important issue. In fact, within the European Union, criminalisation of acts of legal entities is an important and very controversial theme, and it is therefore in the framework of the Council of Europe. Both of the perspectives of the European Union and of the Council of Europe include, at least, any kind (criminal or not) of responsibility of companies and other legal entities by criminal acts of their representatives, acting in their representation and interest. In addition, the Convention states that responsibility of legal entities occurs also in case of lack of supervision or control of a legal representative of the company or other legal entity over someone under its supervision. Some countries in Europe prefer civil remedies, rather to criminal solutions, to regulate the responsibility of a legal person.

Slide 32	**Part Two - National Substantive Criminal Law**
Slides 33 to 43	Trainers will insert here references to national legal provisions.
Slides 44	**Part Three - Case Studies**
Slide 45	**1. Case Study 1** ▪ **Facts / scenario** Bobby is a Police Officer. One night he is on duty and sees a Mercedes parked outside his house. He does not recognise the car but suspects that it belongs to his wife's boss. He phone's into the police station and asks Mary the computer operator to tell him who owns the Mercedes saying that the car had just driven through a red traffic light. Mary confirms that the car does indeed belong to his wife's boss. *Has Bobby committed a criminal offence?* ▪ **Issues** *Has Bobby accessed a computer system?* *Was that access without right?* ▪ **Points for discussion** The computer was accessed by Mary not Bobby she has is authorised to access the data on the computer, she is innocent. It was Bobby who, acting through an innocent agent caused the data to be accessed. He lied to Mary (an illustration of social engineering) does this amount to access in law? Both Bobby and Mary have the right to access the Police computer but subject to strict conditions relating to a legitimate query in connection with police activity. Where the access exceeds this authorisation does this constitute an offence? What if Bobby goes into the police station and manages to look over Mary's shoulder (shoulder surfing) whilst she is making a legitimate enquiry in relation to the ownership of the Mercedes? The 'shoulder surfing' has resulted in Bobby gaining access to computer data. There may be a question as to his 'intention' and of course he has not manipulated the computer system in order to gain access but he has still obtained access without right (though this would be very difficult to prove). This case study is designed to have delegates consider the question of authorisation (access without right). The delegates could also be asked to consider the position had Bobby gone into the police station and looked up the information as to the ownership of the Mercedes on a card index system – the information being the same as that held on computer? The point here is that it is not the data itself that is

	protected (though that may be protected under other data protection legislation whilst Bobby's misconduct might also constitute an offence) rather it is the medium on which that data is stored that is being protected. Police computer systems hold vast amounts of personal information relating to individuals along with a lot of sensitive information. Access to such data should only be granted to those who have a legitimate interest in it. In the UK police officers and police computer operators are frequently found illegally accessing police systems for purposes of their own e.g. to find information that might be interest to the press or in the case of corrupt officers to discover what information is held on a particular person or whether a particular person or group are under active investigation.
Slide 46	**2. Case Study 2** ▪ **Facts / scenario** A security guard at a bank is approached by a group of criminals who ask him to place a device known as a key logger onto the back of a number of terminals in the bank. The key logger records the keystrokes of the user and captures passwords and other information that would enable someone who had access to the terminal to log into the user accounts of bank staff. An additional feature of the Key Logger device enabled it to record Skype phone calls made by the user of the terminal. The criminals also placed a bug on the desk which picked up sound, including all phone calls made and received by the user of the terminal. *Has there been an illegal interception?* ▪ **Issue** *Has there been an interception?* *Has that interception been achieved by technical means?* *Has data been transmitted to or from a computer system?* ▪ **Points for discussion** The key logger is a technical device that is capturing data transmitted from the terminal. This amounts to an interception and is clearly without right. What about the Skype calls? In this scenario it appears that the data travels on the same line as other data transmitted from the computer but what if the user had a stand alone Skype phone? Would such a phone constitute a computer system. The convention defines a 'computer system' *any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*; and 'computer data' *as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*. The use of the audio bug may be a little more difficult. Is it an 'interception'? In the UK the courts have held that for an interception to have taken place

	there has to be some sort of interference or abstraction of the signal whilst it was being transmitted on the network, here the recording takes place independently of the transmission notwithstanding that the same information is obtained had the device been placed on the 'line'. What if the key logger was placed on the system by the Company who are anxious to ensure that their employees are not using the internet for an inappropriate purpose? Most telecommunications systems travel on both public and private networks. At the point where the communication leaves your property it moves from a private system to a public system. The controller of a private system has the right to access communications using that system; so for instance, you would be able to monitor conversations on your home telephone line provided that whatever technical device you used in order to do so was connected to the private side of the system. This scenario is designed to have the delegates consider each of the elements of interception, that there is an interception of computer data in the course of its transmission by technical means without right. The delegates should be clear that this provision is designed to protect the contents of communications rather than information connected with the addressing of the message or the cost of the service.
Slide 47	**3. Case Study 3** ▪ **Facts / scenario** A criminal gang communicate using a web based e mail system that can be accessed through the internet anywhere in the world. Rather than send each other messages that might be intercepted by the police or which may incriminate them if found on their computer they use a 'dead letter drop' system. What they do is write their message as a draft which is never sent, other members of the gang have the password which enables them to access the e mail account and read and respond to the message. If the police were able to access the draft e mail box would this amount to an interception? ▪ **Issues** *Is the message being transmitted?* ▪ **Points for discussion** Most states require the police to establish a high threshold of suspicion before authorising the interception of the contents of a communication. Obtaining evidence without the requisite authority may result in the case being stopped or the evidence being inadmissible. Computers and the internet facilitate a number of different forms of communication, e.g. e mail, instant messaging, twitter, etc. Messages will

	frequently be stored before they are retrieved by the intended recipient. Is a message that has yet to be retried still to be regarded as being in the course of its transmission? There is no way of knowing whether the draft message has been read by the intended recipient. Should the law grant the same protection to those who deliberately choose to subvert the normal means of sending communications by e mail as it gives to those who use e mail as it was designed to be used? This is a fairly common way for criminals to communicate with each other. Whether seeking to access such messages in an interception or not will depend on domestic legislation and or the attitude of the domestic courts but it may be worth delegates realising that if they need to rely on Mutual Legal Assistance to obtain such data the requested state may consider it an intercept or at the least because access to the contents of a communication are being sought will have a higher legal threshold that needs to be established in order to obtain the necessary judicial authority .
Slide 48	**4. Case Study 4** ▪ **Fact/ scenario** Police Officer Bobby has taken his wife's phone, guessed her password and listened to a stored voice message that she has not yet retrieved. *Is this an interception?* ▪ **Issues** Is the voice message still in the course of its transmission? Has there been an interception of computer data? ▪ **Points for discussion** Until the message has reached its destination it is probably still in the course of being transmitted even though it is stored within the system. The message is probably being digitally stored on the phone companies' server and thus Bobby has accessed computer data. Is a phone a computer? Probably yes, it undertakes the automated processing of data. Police officers conducting searches who find phones may need to consider this in order to ensure that they have the necessary authority to access such messages. It would be different if the recipient had listened to the message and opted to store it. This scenario raised similar issues to the previous scenario. It serves to illustrate what might be a fairly common situation that can equally apply to officers who executing a search warrant seize a computer which contains both opened and unopened e mail. It also serves to illustrate that the offence established under Article 3 applies to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.
Slide 49	**5. Case Study 5** ▪ **Facts/ scenario** Bobby is interested in UFOs and he believes that the Russian Government has

captured an alien space craft that landed in Siberia in the early part of the 20th Century. He visits a Russian Military recruitment site which has a link to a site operated by the Russian Air force. The Air Force site requires a password but using a password cracking tool he manages to gain access. He spends some time exploring the system and copies a number of files. He also tries to delete all of the log files of his activity in order to prevent the Russians from identifying him. He then alters the front page of the site so that it displays a picture of a UFO instead of the Air Force insignia .
Has Bobby committed an offence?

- **Issues**

Can unauthorised access of itself amount to an offence of Data or System Interference?

Does erasing the evidence of unauthorised access amount to an offence?

Does serious harm have to be caused to the operation of the computer before criminal liability is incurred?

- **Points for discussion**

The aim of these provisions is to provide computer data and computer programs with protection similar to that enjoyed by corporeal property against intentional infliction of damage.

Bobby was not authorised to access the Air Force site, it was password protected. Access therefore would constitute an offence of illegal access.

Bobby has deleted data , the log files and the Air Force insignia.Though perhaps he generated the log files they are not his, the system was configured to record such activity. He has no right to delete them. The Air Force may wish to know who has access to their system.

By altering the image on the front page he has both deleted and added data to the system which, whilst it is unlikely to have resulted in any important information having been lost, would be an embarrassment to the Air force. However, more importantly though Bobby may claim that he only accessed the system to find information and that he only deleted logs or other data of no importance can any systems administrator have confidence in the integrity of the data following such an unlawful intrusion?

Whether an offence has been committed in these circumstances will be a matter of local interpretation. It may be that the seriousness threshold has not been established. However the systems administrator would probably feel obliged to take the site off line in order in order to establish the effect of the intrusion, particularly if the site that has been accessed contains confidential or sensitive data or is used in operations which, if they were to go wrong would endanger the public such as a system responsible for running a nuclear power station.

	If for the sake of argument the system that Bobby accessed was that used to run a nuclear PowerStation would the offences set out in Articles 4 and 5 be adequate to reflect the seriousness of such an intrusion which amounts to an attack on the National Critical Infrastructure?
Slide 50	**6. Case Study 6** ▪ **Facts/ scenario** An automated spam e mail programme sends unsolicited e mails to thousands of users all around the world every day. If the e mail is opened it downloads software to the user's machine. The software does nothing which affects the running of the users computer, it doesn't acquire data from the users computer nor does it delete any data or cause any other sort of damage, however it means that the users computer is now a 'Zombie' forming part of a 'Botnet' which the 'bot controller' can use to undertake various types of activity. *Has an offence contrary to Article 4 or 5 been committed by the person responsible for sending the spam?* ▪ **Issues** Has there been any unauthorised access to the users machine? Has data been altered on the users machine ? Has there been any damage to the users machine? ▪ **Points for discussion** Even though no damage has been caused the software brings about an alteration of the data on the users computer. That alteration was not authorised as the user was not given any warning or asked to consent in any way to the modification of his computer. Is the sending of Spam itself illegal or is it merely a nuisance? Does it only become illegal when it has an adverse impact? What if the spam e-mail contained an attachment and invitation to the recipient to open the attachment saying "you will like this" ? It might be argued that the recipient has chosen and thereby consented to downloading data to his computer. The reality however is that any consent that may have been given has not been an informed consent though it may be argued that those who choose to open attachments from unknown recipients do so at their own risk. Does it make any difference that the user doesn't care whether their computer became part of 'bot net' or not? As we travel around the internet we visit sites and download data without giving proper consideration to the nature of the material that may be finding

	its way onto our computer but trusting to the names that websites give themselves, the names of files or the results returned by our search engine to make our decisions. Clicking on a thumbnail image of a picture in order to acquire a full size image indicates an awareness of the data that we are seeking to acquire and a fully informed consent as to the nature of that data. Should we click on a thumbnail image of a motor car only to find that the full size image we have acquired is that of an aeroplane we cannot be said to have given our consent to the acquisition of that data. Choosing to open a link to a website will result in a lot of data being downloaded. If the site is a legitimate one the bulk of that data will probably relate to the content of the website though a proportion may consist of advertisements placed by third parties. Again we have made an informed choice and given an implicit consent to receive the advertisement knowing that this is a common practice on the internet. A common practice in the internet industry is to download data to the users internet browser , 'cookies'. Cookies perform a variety of functions including recording a users web browsing history. A user will be given the option to disable the cookie function on the browser, is such an option sufficient to imply that the user has subsequently given their consent to the downloading of such data?
Slide 51	**7. Case Study 7** ▪ **Facts / scenario** Bobby is a former police officer who was sacked for improper use of the police computer system. He decides to get his own back on the police department. He uses an e mail programme which enables him to send 70,000 e mails per hour to his old department. He alters the e mail header to make it appear that it came from the chief officer of police thus fooling the police e mail server into believing that it came from a legitimate source. The police server was unable to handle the volume of traffic and collapsed. *Is this an offence of system interference?* ▪ **Issues** *Sending an e mail involves accessing or seeking to access a computer system, the e mail* server. To what extent does the owner of such a server authorise such access? If you have an e mail address does that not mean that you are inviting others to send you e mail messages? ▪ **Points for discussion** The question is one of right. Bobby has accessed a system and caused the system to collapse by inputting data. By establishing an e mail address which is accessible to the public the owner of the address is implicitly giving their

	consent to the receipt of messages. Bobby might argue that the police have consented to the receipt of each individual e mail and that is not his fault that their system lacked the capability to handle so many messages. But has their really been consent? The owner of a house grants an implied consent for the postman to post letters through his letter box that are addressed to the owner. There is also an implied consent to receive 'junk' mail such as pizza flyers. The homeowner however does not consent to receiving so many pizza flyers that he is unable to open his front door. Might it not also be said that by altering the details of the sender of the e mail access to the e mail server has been gained through fraud? Consent is not given to the receipt of such 'spoofed' e mails. Whilst this scenario concerns e mails the principle is good for those who seek to cause websites to collapse through a denial of service attack whereby the site is unable to handle the volume of traffic directed towards it. Connecting to a website involves the exchange of data between the users computer and the website. Similar issues as to implied consent to connect to the site arise as discussed in relation to email messages.
Slide 52	**8. Case Study 8** ▪ **Facts/ scenario** Bobby sends an e mail to his estranged wife at her place of work. He alters the header to make it appear that it has come from one of her friends. The e mail contains a programme called 'access all areas' which allows Bobby to assume control over his wife's computer. Before Bobby has the chance to use the programme its presence is detected by the system administrator who shuts down the system in order to undertake an evaluation of the extent of the intrusion. *Has Bobby committed an offence contrary to Article 5?* ▪ **Issues** Has Bobby brought about a suppression of data held on the system? Has Bobby hindered the functioning of a computer system? Has any such suppression of data or hindrance to the functioning of the system been without right? ▪ **Points for discussion** The response of the system administrator to Bobby's e mail means that service has been denied to the users of the system. Access to data held on the system has therefore been suppressed, albeit it the restriction on access is likely to be temporary. The offence does not require data to be permanently unavailable. We have discussed the extent to which the owner of an e mail address grants

	consent to the receipt of data from others. Article 5 concerns computer systems, that is one or more computers linked together. Is a lone computer connected to the internet part of a system? Bobby's wife's work computer is more likely than not part of a system , she is probably part of a LAN (Local Area Network) or WAN (Wide Area Network) or Intranet . Has Bobby hindered the working of the system? Bobby might argue that he is not responsible for the denial of service and that he had no intention to bring about such an event, in fact quite the opposite he wanted the system to carry on running so that he could find out what his wife was up to. Frequently denial of service attacks are insufficient to take a website off line , however service providers will take the site offline in order to minimise the effect of the attack on its systems and minimise inconvenience to other customers. In this scenario Bobby does not appear to have the requisite intention for an Article 5 offence though this does not mean of course that he escapes criminal liability. This is an example of a Trojan virus which is a common way for cyber criminals to gain access to the computers of others
Slide 53	**9. Case Study 9** ▪ **Facts/ scenario** An online internet "hacktivist" group who are protesting against the use of animals to test cosmetics undertake "Distributed Denial of Service" (DDOS) attacks against the websites of cosmetic companies , and glamour magazines. Through their website the group distribute software they call the 'Supergun' which enables the group to co ordinate attacks on websites and to thereby maximise the amount of traffic seeking to access a website at a particular time. The 'Supergun' software was originally developed as a tool by systems administrators to test the security of their systems. However whilst the software still works in exactly the same way the user interface has been rendered much easier to use and now bears the logo of the group. *Is it an offence to make the Supergun available for downloading?* *Is it an offence to be in possession of the Supergun?* ▪ **Issues** Does the fact that the Supergun can be used for a legitimate purpose mean that a prosecution cannot be brought? Does making the Supergun available to be downloaded amount to distribution?

	▪ **Points for discussion** The offences to which this Article relates are; unauthorised access, illegal interception, data and system interference. Whilst the software was originally dual use, that is had a legitimate function, now that the user interface has been modified does this mean that its possession etc is an offence? Looking back at our previous case studies, the 'access all areas' software used by Bobby to gain access to his wife's computer has a legitimate use. Programmes such as this allow users to access their own computers remotely What about Bobby's possession of password cracking software; would this be an offence? May be an issue of intent, what legitimate reason does he have to possess such software? Is there any evidence to show that he has sought to deploy this software in order to commit an offence? This offence is not designed to be used to criminalise legitimate software providers and users. Where, as there is here, evidence of a malicious intent the problem does not perhaps arise. However those involved in cybercrime are also frequently involved in legitimate internet activity and may well be industry professionals who use and develop such software but whom , when opportunity presents itself are prepared to deploy it in furtherance of illegal activity . What about shopkeepers? how are they supposed to know what intention a customer might have in relation to a particular piece of hard ware or software. Is the ambit of the offence too vague?
Slide 54	**10. Case Study 10** ▪ **Facts/ scenario** A software provider has produced encryption software. The software divides the contents of the hard drive into two volumes, each requires a password to access however only one volume is visible to the ordinary user and the existence of the hidden volume cannot be detected using forensic software that is currently available. The manufacture claims that this software would be of use to anyone who may find themselves in a situation where they are under coercion to reveal their password. It would mean that the data on the hidden volume can be kept secure even if they disclose the password to the visible folder. ▪ **Issues** Does the manufacture, production, distribution use or possession of such software constitute a criminal offence? ▪ **Points for discussion** We are all being constantly urged to keep our data secure. Whilst such a programme is obviously useful to those engaged in crime and in particular

	those who are fearful that the contents of their computers might incriminate them, the programme is not being used by them to commit an offence rather it is being used to conceal evidence. Cyber criminals may make use of other programmes or systems to avoid detection including anonymizers which enable them to surf the internet without disclosing their true IP address or evidence eliminator programmes which can erase the contents of a hard drive.
Slide 55	**11. Case Study 11** ▪ **Facts / scenario 3** Nick works for in the IT department of a large company which has its own intranet. Company policy forbids its employees from using their companies' computer and internet connection to make online purchases. In his spare time Nick begins to develop software which would enable the company to identify those employees who are making online payments and to capture that information so that it can be used in evidence in disciplinary proceedings. Nick lacks the necessary skills and makes online contact with 'Jupiter'. Together they develop a piece of software that once downloaded to a users computer will activate when that user begins to complete an online, form such as that used to process online payments and will capture the data inputted by the user. Nick's company is very pleased whilst Jupiter begins to deploy the software using a Trojan programme. *Has Nick committed an offence?* *Has the company committed an offence?* *Has Jupiter committed an offence?* ▪ **Issues** Has the device been designed or adapted primarily for the purposes of committing designated criminal offences? ▪ **Points for discussion** Cybercriminals are able to access a variety of tools that enable them to commit offences or which will assist them in doing so. It is possible to purchase the code which will enable you to build your own 'bot' or purchase a 'bot net ' or to purchase access to a bot net which will enable the user to undertake various types of crime such as 'phishing' . Jupiter will use this programme to obtain financial information from users which can be exploited by either Jupiter himself or others. The company presumably thought that Nick had produced this during the course of his employment. Nick is innocent and has inadvertently helped Jupiter create a powerful criminal tool. Neither Nick nor the Company have the requisite criminal intent. Would it be different if Jupiter went on to market the programme to other companies who wished to monitor their employees

	internet activity? Could Jupiter argue that the software has a legitimate purpose despite its obvious attraction for criminals?
Slide 56	**12. Case Study 12** ▪ **Fact / Scenario** Stefan uses a commercially available photographic software to produce a realistic bankers draft on his home computer. He takes the draft to his bank who accept it as genuine and transfer funds to Stefan's account. *What offence has Stefan committed?* ▪ **Issues** Is the production of the forged bankers draft a computer related forgery? Is the offence only completed once the bank clerk accepts the draft as being genuine? ▪ **Points for discussion** Creating the bank draft involves inputting inauthentic data into a computer, i.e. that the draft has been made out in favour of Stefan. However has this been done without right or has Stefan the right to produce such a document on his own computer? Stefan may have the intention to use the draft to defraud the bank but, for whatever reason may never get around to printing the draft. Does it make a difference to Stefan's liability whether the document is ever produced on paper? This offence was not really created to deal with this type of scenario though it may serve if domestic legislation would not otherwise criminalise the production of a forged banker's draft These offences may better be considered in terms of secondary liability such as attempt. This offence is really aimed at those who use a computer as the mechanism to commit the offence, thus when acting in good faith the bank clerk inputs the data supplied by Stefan accepting that the data is authentic.
Slide 53	**13. Case Study 13** ▪ **Facts/ scenario** Stefan has always boasted to his friends of his prowess as an athlete when in his teens. His friends are sceptical. He manages to gain access to the database of his old school and alters the records to show him as captain of the school athletics squad and him having won a number of medals. *Is this an offence of computer related forgery?* ▪ **Issues**

	The data that has been altered will not be acted upon for any legal purpose. ▪ **Points for discussion** Stefan has altered data and inputted inauthentic data. It is clear that this access and alteration is without right. Leaving aside the other offences that Stefan may have committed it is doubtful that he has committed a computer related forgery as this data will not be acted upon for legal purposes. The forgery related offence is not concerned with financial or other gain; those offences come within the ambit of computer related fraud. This Article seeks to ensure the security and reliability of electronic data which may have consequences for legal relations. The term "for legal purposes" refers to transactions and documents which are legally relevant.
Slide 58	**14. Case Study 14** ▪ **Facts / scenario** Now that he has lost his job in the Police Force and is having to pay alimony to his wife since their divorce Bobby is looking for another way to make money. He has always had an interest in share dealing and purchases 1000 shares in Flanders Mining Inc a company with an exclusive right to mine uranium in Belgium for 1 euro apiece. Bobby is a member of an internet forum whose members are, like Bobby, interested in the stock market. Bobby posts a message saying that a friend in the Belgium government has told him that substantial amounts of uranium have been detected in Belgium. Following this announcement the share price in Flanders Mining takes off, by the end of the week each share is worth 1000 euro. Bobby then sells his shares. *Has Bobby committed an offence?* ▪ **Issues** Is Bobbie's message untrue? If the message was untrue has another person lost property as a result? Has Bobbie gained an economic advantage? ▪ **Points for discussion** If the message posted by Bobby is untrue then he may have committed an offence. He has inputted false data into a computer and has gained an economic benefit for himself in the rise in the share price. Is the causal connection between the inputting of the data and the effect to remote? Has Bobby caused a loss to another? Arguably yes in that the shares are incorrectly valued and will at some point presumably fall. However it has to be recognised that the market for shares is extremely volatile, is not the value of a

	share the price that anyone is willing to pay for it at any particular time? Has anyone really been defrauded, are these types of rumours and messages not rife on the internet? is anyone really going to believe this post or fail to see it as a clumsy attempt to manipulate the share price ? Does this mean that we cannot tell lies on the internet?
Slide 59	**15. Case Study 15** ▪ **Facts/ scenario** Stefan drives to the bank. In the car park he finds that he is short of change. He puts a washer into the automated parking machine and obtains a ticket. *Has Stefan committed an offence?* ▪ **Issues** Is the parking machine a computer? Does it matter that the parking machine produces tickets automatically and no human being has been deceived? What is the status of the parking ticket? ▪ **Points for discussion** The parking machine is a computer, it processes data calculating the amount of money tendered against the parking tariff and issuing a ticket for the appropriate length of time. Stefan has inputted inauthentic data, the washer rather than the appropriate coin. Article 7 does not require a human to have acted on the data supplied. The parking ticket is a forgery, the data used to create it was false and it was produced in order that a person, the car park attendant, would regard it as genuine and not give Stefan a parking ticket.
Slide 60	**16. Case Study 16** ▪ **Facts / Scenario** After his arrest the police discover that Stefan is in possession of the credit card details belonging to a large number of third parties. *Is the possession of this data a criminal offence?* ▪ **Issues** What status do computer files have? Are they 'things' in law despite the fact that all they consist of is a string of binary code? ▪ **Points for discussion** In the UK it is a substantive criminal offence to be in possession of an article for use in fraud. Article includes a computer file. Of course it is necessary to prove the necessary intent but it is difficult to argue a legitimate reason to have possession of data of this type. It may be that this might be regarded as a preparatory offence.

Slide 61	**17. Case Study 17** ▪ **Facts/ scenario** Adam is a member of an exclusive online group who exchange photographs of children being sexually abused. Adam is also a member of a 'peer to peer' file sharing group, he places photographs of children being abused that he has obtained from the online group into this peer to peer shared folders which makes it accessible to others on the peer to peer network. *What offences has Adam committed?* ▪ **Issues** Definitions of production, procurement and distribution. Adam has downloaded image files from the internet. Does downloading equate to the production of such an image? Downloading, and particularly saving an image on a computer is not like watching TV. The act of downloading creates a new thing , a computer file thus viewing images on the internet involves the making of new images. Prosecutors may find this concept useful. Peer to Peer file sharing networks allow members to access files made available to them by other members of the network . By placing the images into the shared folder Adam is making them available for distribution.
Slide 62	**18. Case Study 18** ▪ **Facts / scenario** Bill is arrested at the airport on his return from Cambodia . His laptop is found to contain a large number of images of him engaged in sexual activity with children who appear to be from South East Asian. *Can Bill be prosecuted in respect of the images?* ▪ **Issues** Jurisdiction. Choice of substantive offence, being in possession of an image or making the image. ▪ **Points for discussion** There may be jurisdictional issues in relation the making of the images as these appear to have been produced overseas. Possession should not be a problem.

	What would the position be if all of the images were found on unallocated space? Possession requires both knowledge and control. Bill may or may now know that images which are deleted may still be accessible on the hard drive, however unless he has the technical means and expertise he will never be able to recover them. However it remains (subject to jurisdictional issues) for a prosecutor to either prosecute for making the image or for being in possession of the images in the past . What would be the position if the images were of nude children aged 3- 7 playing on a beach and Bill explains that he is a naturist but accepts that he obtains sexual gratification from looking at the images? Whether such images are illegal is a matter for local interpretation. In the UK we generally require images to have sexual element and we would regard the motivation of the photographer as being irrelevant. *Who decides which image is illegal? Is the ambit of the offence sufficiently clear?*
Slide 63	**19. Case Study 19** ▪ **Facts / scenario** WWW.Iuvfishin.com is a Website devoted to fishing. The site is hosted on servers located in the USA The owners of the site discover that it had been hacked and that a thousand child abuse images have been uploaded and embedded within the site. The way it has been done means that these images would not be visible to ordinary users of the site. The site logs the IP addresses of those who have accessed the photographs. An IP address attributed to John has been given to the police in your country They search John's address and seize his computer which contains thousands of child abuse images. It is clear from the internet history and the data within these files that most of the images have been downloaded from the internet. ▪ **Issues** How to prove that John is responsible for the images? The impact on suspects accused of paedophile offences**.** ▪ **Points for discussion** This method of concealing images is not uncommon. Groups will post links to the images. However, it may be dangerous to rely on the IP address alone to obtain a search warrant without understanding how that IP address came to be logged on the site , they could have got their entirely innocently having been referred by another site and not gone on to access any images once they realised what they were . Of course they may have visited on more than

	one occasion or accessed a number of images. Can use this to discuss the care needed before accusing ain individual of being a paedophile. There is a high rate of suicide amongst persons accused of these offences. As in all cyber crime cases you need to be able to put the suspect at the keyboard at the relevant time , an IP address may be used by a number of individuals at the same address or the wireless network may have been hijacked by someone else. Accusations of this type can have a devastating effect on an innocent individual.
Slide 64	**20. Case Study 20** ▪ **Facts / scenario** The police in the USA have taken down a website that hosts sites offering child abuse images for those who pay a monthly subscription. The USA authorities have captured data from those who have paid for access, including IP address, credit card numbers, e mail address, billing address and password. One of the customers is Oswald. Having obtained a search warrant his computer is examined. Nothing incriminating is found because Oswald has used a programme called "Elimination of Evidence" *Has Oswald committed an offence?* ▪ **Issues** Has Oswald committed a substantive offence or one of secondary liability? Are there issues about jurisdiction? Does it matter that the US website was fully automated? What do we say about the use of the Evidence Elimination programme? ▪ **Points for discussion** Oswald is not in possession of any images and we cannot prove that he ever accessed a website to view such images albeit that we can prove that he paid a subscription in order to do so. However Oswald has paid money in order to persuade another person, the website owner in the USA to distribute or make available child abuse images for distribution. Does this therefore constitute an offence? That the US website if fully automated means that no human being is actually involved in the processing of the credit card details. Even so, the process was created by and is administered and maintained by a person who is profiting financially. The use of an evidence elimination programme is not, per se illegal. Unless Oswald was able to activate the programme during the course of the police investigation he is unlikely to have committed an offence connected with the

	administration of justice. However if Oswald is prosecuted the use of such programmes may be regarded as an aggravating feature by the court.
	Practical Exercises (if applicable) No practical exercises are prepared for this session
	Knowledge Check The trainer should check knowledge by asking relevant questions from each of the session aspects.
Slides 65 and 66	**Summary / Recap** The trainer should recap / test knowledge on the following points: ▪ The substantive criminal law provisions and some of the key factors used to describe the crimes, based on the Convention of Budapest. ▪ The substantive criminal law provisions and some of the key factors used to describe the crimes, based on the existing national law. ▪ The needs and the advantages of the harmonisation between national legislation and the international instruments, in particular the Convention of Budapest. ▪ The relevant substantive law provisions from case study discussions

6.6 Lesson 1.2.4 Procedural domestic law	Duration: 90 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation

Aim:

The purpose of this session is introducing the participants of each country to investigative measures provided for by national law and national regulation on electronic evidence.

Objectives:

By the end of the lesson the students will be able to:

- Identify national regulations on electronic evidence
- Identify the investigative measures allowed under national law and the value and requirements of gathering and preserving electronic evidence
- Identify some specificities of the national proceedings, regarding electronic evidence, in the context of the international legal framework scenario

Introduction

This session has been prepared to provide students with an example of how the Budapest convention has been incorporated into the national legislation of one country, in this case Portugal. Trainers will need to replace the Portuguese information with the corresponding legislative details from their own country.

Slide nr.	Content:
Slides 1 to 29	**PowerPoint (or other type of presentation)** The content of the slides in this section are example of what can be described in each of the local trainings. Ideally, the session on electronic evidence should mention the international legal instruments signed or ratified by each State and the result of its transposition to the domestic law. Besides, a description of the types of investigative measures allowed under national law, as wellas an explanation on the importance and requirements of gathering and preserving electronic evidence should be provided. At the end, if applicable, eventual specificities of the national proceedings regarding electronic evidence should be mentioned.
Slide 2	**Agenda** This presentation has three parts: ▪ Part One will refer to the procedural provisions of the Budapest Convention; ▪ Part Two, will provide a description of the procedural provisions under the national law;

	▪ Part Three will provide a summary of the two previous parts.
Slide 3	By the end of this session delegates will be able to explain the procedural provisions of the Budapest Convention and to explain the existing procedural provisions under their domestic law.
Slide 5	**Part One - Procedural provisions of the Budapest Convention** One of the most important aspects of the Convention, which must be strongly underlined, is its procedural dimension
Slide 6	Article 14 opens up the Budapest Convention to very broad scope. According to it, the Convention will be applicable – obviously -, when the crime under investigation is one of the offences listed in the Convention. However, but it also includes two extremely far reaching extensions: ▪ procedural rules can be used in the investigation of any crime if it was committed by the means of a computer system; ▪ the rules also apply to the gathering of electronic evidence in relation to any crime. This means that every crime potentially falls under the procedural rules of the Cybercrime Convention.
Slides 7 to 10	Articles 16 and 17 describe the expeditious preservation of computer data and expeditious preservation and disclosure of computer data. Both provisions are very innovative and extremely significant. Traditional pieces of evidence will stay on the crime scene, eventually, for a long period of time, but digital data – electronic evidence – is very volatile and may disappear very quickly. Article 16 therefore introduces "expedited preservation" as an immediate provisional measure to keep evidence and give time to obtain judicial orders for the seizure or disclosure of the data. This may be traffic data or content data. A communication on the Internet may not only involve one but several service providers. It is important that law enforcement is able to order any provider along the path of a communication to preserve the data wanted. Therefore, under Article 17, a service provider may be ordered to disclose a sufficient amount of traffic data to determine the path of the communication. Articles 16 and 17 refer to specific data needed in a specific investigation. This is not to be confused with data retention regulations that require providers to keep all traffic data for a certain period of time in case this is needed by law enforcement. The Budapest Convention does not have such a data retention provision.
Slides 11 to 13	The provision of Article 18 is also very interesting. According to it, each Party must adopt legislative measures to empower its law enforcement authorities with the possibility of giving "production orders". This judicial order can be

	issued by law enforcement agencies to citizens and to Internet service providers, ordering them to provide the competent authorities with data stored in a computer system, under their responsibilities or provide subscriber data. According to the Convention, the production order must specify the nature and extent of the required data: it is very clear that the data required by the investigation must be previously determined; *fishing expeditions* are therefore prohibited. The purpose of this legal limit is to prevent abuse of these new investigative powers by law enforcement agents. In the real world, a search or seizure of objects or documents is normally only directed to objects or documents directly related to a case under investigation. In the digital world, if the rule was the complete permission of access to the whole information that comes with a piece of hardware, it would be permitted to access all kinds of information stored on that computer, often unrelated to the crime under investigation and (e.g. in the case of email communication) involving also third parties. If Article 16 is the first step (preservation of data), Article 18 is the 2nd step when the data preserved have to be disclosed to the authorities.
Slides 14 to 19	Search and seizure are described by Article 19 of Budapest Convention. Most of national procedural rules include general regulations for search and seizure, but not all of them have specific rules governing computer search and computer seizure. Many jurisdictions can live well just with traditional searches and seizures. However, the real world teaches that digital investigations face challenges previously unknown caused, for example, by the interconnectedness of computer systems. Enfacing that kind a new questions, Budapest Convention created specific rules to deal with searches and seizures in the digital world. For example, there is a specific rule, in Article 19.2, relating to the hypothetic extension of a search when, during a search of a computer system, the investigators conclude that there is a need to extent that search to another computer system. Under the Convention, when an authority lawfully gains access to a specific computer system or part of it, and in the course of inspecting this system form a reasonable belief that the data sought is stored in another computer system in its territory, that authority can "expeditiously" extend the search to the other system. Specifically with respect to seizures, there are some concrete topics that must be underlined because they are typical for the new digital environment: the various possibilities of physically seizing computer data. As most of the legislations just have specific regulation to searches in the physical world, they don't have special regulation to the new and more efficient ways that are available to seize computer data.

	In particular, the Budapest Convention demands that signatory states enact enabling legislation that allows during the process of a lawful seizure of computer data to: a) seize physically a computer system, b) make and retain a copy of those computer data (which is important in case the data is stored on a major server, where physical removal is impossible, and also when physical seizure would interfere too significantly with the rights of other people who have access rights to that machine – for instance the a big company's server) c) maintain the integrity of the relevant stored computer data and, finally, to d) render inaccessible or remove those computer data in the accessed computer system. This last provision is relevant for instance when physical seizure is impossible, but real harm could ensue if a third party got access of the data. With the exception of the mere seizure of data in its own and original record, all these procedural possibilities are specific measures from the digital environment.
Slide 20	Sometimes, the investigator needs more recent information, rather than the information already stored on a computer system. The *real-time* collection of traffic data allows live investigations and is described in Article 20 of the Budapest Convention. Such kind of intrusive measure requires proper legislation to allow law enforcement authorities to collect or record, through technical means, data in real time, and also the power to compel service providers to collect or record traffic data from their costumers, within its normal activity, in real time. This kind of investigative tool can be very important, for example, to establish the source of a communication, in view of identifying a perpetrator, in real time.
Slide 21	Last, but not least Article 21 describes interception of content data. Besides of traffic data, sometimes, law enforcement authorities need to know the real content of communications between suspects of a crime. Some countries already have provisions on telephone interceptions, but not all of them allow the authorities to, specifically, intercept communications, other than by telephone. That is the reason why, on Article 21, specifically, Budapest Convention includes provisions that enable investigators to intercept and record data communications. Besides being a very powerful investigative tool, the interception of communications is also a very intrusive measure and is only allowed, by the terms of the Convention a range of serious offences to be determined by national laws.

Slide 23	**Part Two - Procedural provisions under the national law**
Slides 24 to 31	Trainers will insert here references to national legal provisions.
	Practical Exercises (if applicable) No practical exercises are prepared for this session
	Knowledge Check The trainer should check knowledge by asking relevant questions from each of the session aspects.
Slides 33 to 34	**Summary / Recap** The trainer should recap / test knowledge on the following points: ▪ Describe national regulations on electronic evidence ▪ Mention the international framework, if applicable ▪ Discuss the types of investigative measures allowed under national law and the value and requirements of gathering and preserving electronic evidence ▪ Identify some specificities of the national proceedings regarding on electronic evidence, in the context of the international legal framework scenario

6.7 Lesson 1.3.1 Daily Review	Duration: 30 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation

Aim:

The purpose of this session is to review the previous days activities, obtain feedback from the delegates and check that the objectives of the sessions have been met

Objectives:

By the end of the lesson the students will be able to:

- Identify areas of the previous days activities that they have understood
- Identify such areas where they need to review the materials to bring their knowledge to the required level

Introduction

This session has been prepared to allow students to check that they have understood the previous days teaching and that they are able to meet each of the objectives for the individual sessions. It is also to provide the trainer the opportunity to check the knowledge level of the students and to identify areas where the teaching materials may be improved.

Slides nr.	Content:
Slides 1 to 12	**PowerPoint (or other type of presentation)** The slides in this presentation are provided to assist the trainer and the delegates with the previous days activities. The trainer should recap on those activities using the agendas and objectives as the benchmark.
	Practical Exercises (if applicable) No practical exercises are prepared for this session
	Knowledge Check The trainer should check knowledge by asking relevant questions from each of the session aspects.
	Summary / Recap This whole session is designed as a recap of the previous days activities and no separate recap is required

6.8 Lessons 1.3.2 & 1.3.3 Electronic Evidence	Duration: 120 & 90 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- Internet access (if available)
- PowerPoint Presentation
- Computer hardware examples (if available)
- Copy of the EC OISIN funded e-evidence guide

Aim: The aim of this session is to provide judges and prosecutors with the knowledge of issues relating to electronic evidence such as the various types that they may encounter, how it is recovered and handled during investigations and produced for criminal trials. Further knowledge about the challenges of retrieving such evidence from other jurisdictions is also provided.

Objectives:

By the end of the lesson the students will be able to:

- Discuss various types of electronic evidence
- Explain the principles of best practice relating to the seizure and handling of electronic evidence
- Identify the challenges offered by "dead box", "live data" and Internet sources of electronic evidence
- Identify the challenges of obtaining evidence from another jurisdiction
- Discuss the issues of admissibility of electronic evidence in judicial proceedings, in terms of its authenticity, accuracy, completeness

Time	Content:
30 minutes 30 minutes 60 minutes 60 minutes 30 minutes	▪ Introduction and opening (Agenda and Session objectives) ▪ Part 1 – What is electronic evidence ▪ Part 2 – Procedures and Good Practice ▪ Part 3 – Legal Issues ▪ Summary/Recap

Introduction

This session is intended to provide trainers with a framework for developing training material to be delivered as part of a wider programme. It cannot be comprehensive as technology changes so rapidly that any detailed technical specifications would be out of date almost as soon as the document is published. Ensuring that Judges and prosecutors have sufficient understanding of technical issues as they relate to matters before them is essential to the fair running of any judicial system. This session provides an overview of the relevant aspects of technology and its relevance to the criminal justice system. A PowerPoint presentation is provided as a resource for trainers to use if considered appropriate.

This session provides information about technology that will be encountered by Judges and prosecutors during their work and which is used by criminals to commit crime and law enforcement to detect it.

This session has relied on the document "seizure of e-evidence" for much of its source material. This document was created with funding from the European Commission under its OISIN programme under reference 2002/OIS/014[3]. This document was created several years ago and parts of it are therefore dated. Where relevant, the information in it has been updated for inclusion in this training course. The document was produced primarily for the Law enforcement community; however others may apply the principles and procedures in the criminal justice system. This document can be applied to all cases in which e-evidence should be seized.

Each Member State should take its own legal documents and regulations into consideration when interpreting the measures proposed in this document. In addition, each Member State should add its own expert units' contact information.

An organisation or agency wishing to apply the recommended procedures should determine the responsibilities for individual steps/actions according to its internal structure.

Slides nr.	Content:
Slide 1	**PowerPoint** (or other type of presentation)
Slide 2	**Agenda** The agenda slide lists the parts of the session and the trainer should go through these elaborating where necessary on specific aspects that have emphasis for particular groups of students. The trainer should explain how the materials will be delivered and that there will be time for interaction and questions. The trainer should emphasis that this training is designed to be interactive and that delegates will be expected to participate throughout. The trainer should explain whether there is an assessment and what form that would take, including details of any pass mark that is applied. (For this pilot programme, no assessment is included).
Slide 3	It is important that the delegates should understand what the objectives of the lesson are. These should be "SMART" objectives and explained in detail to the delegates before the session begins, using the information on the slide.
Slide 6	**Part One – What is electronic Evidence**
	Types and sources of electronic evidence **Examples** The trainer should begin a discussion with the group by identifying types of electronic evidence and encouraging the participants to give details of their knowledge of the issue. The trainer should then list the types highlighted on

3 http://register.consilium.europa.eu/pdf/en/03/st14/st14583.en03.pdf

	a flip chart or white board. The trainer should complete the list if the audience does not highlight particular types of evidence. The list should include both types of evidence e.g. dead box, live data, memory, Internet, as well as sources of evidence such as those dealt with in the technology section of the course.
Slide 8	**Definition** The definition of evidence is normally prescribed in national legislation. As this is an international course a generic definition has been used. This is from Black's Law Dictionary. Trainers should replace this with national definitions when delivering this course in country. "Evidence is 'any species of proof, or probative matter, legally presented at the trial of an issue, by the act of parties and through the medium of witnesses, records, documents, exhibits, concrete objects, etc. for the purpose of inducing belief in the minds of the court or jury as their contention.' Electronic information generally is admissible into evidence in a legal proceeding".
Slides 9 and 10	There is no internationally accepted definition of electronic evidence. However, in all countries there are regulations containing precepts which, in some way, refer to *electronic evidence.* One useful example of a "definition" is: Information or data of investigative value that is stored on or transmitted by an electronic device. www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm Once again it is the responsibility of the trainer to ensure that any national definition that may exist is included in the course for in country training. Combating modern forms of criminality requires the support of experts and specialised officers ▪ To analyse the evidence and to correctly interpret it ▪ During investigations and the trial phases
Slide 12	**Sources and types of electronic evidence** It is not necessary to revisit the entire lists of types and sources of evidence that were identified in the technology section of this course. The trainer should recap using the list that was created at the beginning of this session. Sources cover any electronic device. The trainer may wish to identify at this stage the importance of electronic evidence from different devices and the role they have played in cases. The types of evidence to be covered are those involving:

	▪ Static Data ▪ Live Data ▪ Internet Data
Slide 13	**Features of electronic evidence** There are many features of electronic evidence that create additional challenges to its admissibility than traditional evidence. In most instances it is dealt with and handled in the same way as other evidence and it is the understanding of the issues that arise and the ability of judges and prosecutors to relate to the electronic nature of the evidence that is the key factor. As may be seen from the examples provided in the course, many of the issues listed relate to both electronic and traditional evidence; however there are some differences and these should be highlighted at this stage. The issues are: ▪ **Volatility** - Can be changed easily - May not be available for long ▪ **Nature** - May require specialist skills to access - May require expert evidence to interpret it - May need to exercise coercive power to obtain and access or use may be restricted ▪ **Location** - May be inextricably linked to non evidential material - May be outside the jurisdiction ▪ **Volume** - Identifying evidential material - Identifying unused material
Slide 14	**Evidential Issues** The features of electronic evidence lead to several issues that should be highlighted. The trainer with the use of examples should elaborate these on. The issues are: ▪ Hearsay ▪ Business records ▪ Automated processes ▪ Intermingled evidence ▪ Data Volumes ▪ Expert evidence ▪

	▪ **Fragile.** Some digital data processed by a computer system is highly fragile and can easily be deleted or modified. This aspect is not only relevant for the evaluation of the digital evidence but also for the process of collecting it. Data that is solely stored in the RAM system memory will in general be lost if the system is shut down unless special technical measures to prevent this process are applied. As the information stored in the system memory can be of great importance for an investigation, the technique of collecting this evidence can be different from processes of collecting traditional evidence. ▪ **Susceptible to alteration.** Digital data is susceptible to alteration. One of the most fundamental principles of computer forensics is the need to maintain the integrity of the digital evidence. Ensuring a full documentation of the process and the application of methods to maintain the integrity of computer data is essential to avoid the suspect claiming that the evidence was tampered. As a result, computer forensic experts seek to substitute investigation processes that lead to an alteration of files on the suspect's computer by more sophisticated processes. ▪ **Decentralised storage.** The availability of broadband access and remote storage servers has influenced the way in which information is stored. While in the past investigators were able to focus on the suspect's premise while searching for computer data, today they need to take into consideration that digital information might physically be stored abroad and only remotely accessed by the suspect if necessary. ▪ **Speed of the technical development.** Technical development is continuing at a fast pace. A significant number of developments post new challenges with regard to forensic examination. This development requires constant training of those who are involved in the collection of evidence, as well as keeping the forensic equipment up-to-date. New versions of operating systems and other software products might generate different data that could be relevant for investigations. Similar developments take place with regard to the hardware. While in the past data was stored on floppy disks, the investigators today have to take into account that relevant information might be stored in MP3 players or watches that include a USB-storage device.
Slides 18 and 19	**Part Two – Procedures and Good Practice**
	There is heavy reliance on the issues dealt with in the e-evidence guide in this part of the lesson. Many details are provided to assist the trainer to build the lesson. These are detailed in the trainer guide and are summarised by bullet points in the associate slides. The trainer should consider how much detail is necessary based upon the requirements of the delegates to enable the

	objectives to be met. The guide may be applied to all cases in which electronic evidence should be seized. Each Member State should take its own legal documents and regulations into consideration when interpreting the measures proposed in this document. In addition, each Member State should add its own expert units' contact information. An organisation or agency wishing to apply the recommended procedures should determine the responsibilities for individual steps/actions according to its internal structure.
Slide 20	**GENERAL PRINCIPLES** When handling e-evidence, it is crucially important to follow the general principles, i.e., 1. On site witnessing, 2. Data integrity, 3. Audit trail, 4. Expert support, 5. Officer training, and 6. Legality and adherence to principles. The principles are explained in the following sections.
Slide 21	**1. On Site Witnessing** Principle: *The officer in charge should never attend the scene alone* At least two officers should be involved in this type of activity. This provides self-protection on the one hand, and helps to catch more details at the scene on the other. The officers should plan and coordinate their actions. If unexpected problems occur, it is easier to solve them because "two heads are better than one".
Slide 22	**2. Data integrity** Principle: *No action taken by law enforcement or their officers should change electronic devices or media which may subsequently be relied upon in court* When handling electronic devices and data, they must not be changed, either in relation to hardware or software. The officer in charge is responsible for the integrity of the material recovered from the scene and thus for commencing a forensic chain of custody

Slide 23	**3. Audit Trail** Principle: *An audit trail or other record of all actions taken when handling electronic evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result* It is imperative to accurately record all activities to enable a third party to reconstruct the first responder's actions at the scene in order to ensure probative value in court. All activity relating to the seizure, access, storage or transfer of e-evidence must be fully documented, preserved and available for review.
Slide 24	**4. Expert Support** Principle: *If it is assumed that electronic evidence may be found in the course of a police operation, the officer in charge should notify experts/external advisers in time* For investigations involving search and seizure of e-evidence it may be necessary to consult external experts. All external experts should be familiar with the principles laid down in this or similar relevant documents. An expert is supposed to have: ▪ Necessary specialist expertise and experience in the field, ▪ Necessary investigative and legal knowledge, ▪ Necessary contextual and legal knowledge, and ▪ Appropriate communication skills (for both oral and written explanations).
Slide 25	**5. Officer Training** Principle: *The first responders must be appropriately trained to be able to search for and seizure e-evidence if no experts are available at the scene* In exceptional circumstances where it is necessary that a first responder collects e-evidence and/or access original data held on an electronic device or digital storage media, the first responder must be trained to do it properly and to explain the relevance and implications of his/her actions.
Slide 26	**6. Legality and Adherence to Principles** Principle: *The officer and agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles, and the above listed principles are adhered to. This applies to the possession of and access to electronic evidence.* Each Member State should take its own legal documents and regulations into consideration when interpreting the measures proposed in this document. One of the internationally important legal documents, the Convention on Cybercrime by the Council of Europe, is currently open for signature by the Member States and the states which have participated in its elaboration, and for accession by other states.

Slide 28	**Types of seizure** The different options for the seizure of electronic evidence are an important aspect of this training course and all have different features, risks and results. The trainer should ensure that these are explained in some detail so that the participants are able to understand the impact of these on their roles as judges and prosecutors. The following information is provided to allow trainers to develop suitable material. There are four general types of e-evidence seizure: 1. Seizure by confiscating electronic equipment and storage media; 2. Seizure by copying the entire memory contents (imaging or mirroring); 3. Seizure by confiscating the backup storage media 4. Seizure by selective data copying; and 5. Seizure of evidence from the internet The different types of seizure are discussed in the following sections. Please note that it is possible to combine different types of seizure within one seizure procedure. For example, it might be necessary to confiscate both the electronic equipment and the backup storage media.
Slide 29	**1. Seizing electronic equipment and storage media** This type of seizure may be suitable in the following cases: ▪ There is not much equipment to be confiscated, e.g., a stand-alone PC or a small network (e.g., in the apartment of a suspect); ▪ There is no risk of a high financial or other loss that may be caused by the non-operation /unavailability of the confiscated equipment; ▪ Confiscation is absolutely necessary due to the nature of the particular offence; ▪ It is necessary/required to stop the activities supported by the equipment to be confiscated. The advantages of this type of seizure are as follows: ▪ It can usually be performed without expert support at the scene; ▪ The seizure procedure is usually not time consuming; ▪ The e-evidence is taken under control; and ▪ The e-evidence can be analyzed in a controlled environment. The disadvantages of this type of seizure are as follows: ▪ there is a risk of damaging the equipment; ▪ there is a risk of harming the persons unrelated to the crime in question; and ▪ there is a risk of interfering with activities unrelated to the crime in question. **2. Copying the entire memory contents** For this type of seizure, sometimes referred to as the imaging or mirroring, special equipment is used to create an exact duplicate of the memory contents of the electronic equipment (or digital storage media) on an external

	storage medium. This type of seizure may be suitable in the following cases: ▪ there is a considerable amount of equipment to be considered (e.g., small- or medium-sized-enterprise); ▪ there is a risk of a high financial or other loss that may be caused by the non-operation /unavailability of the equipment (e.g., the IT system may be considered vital to the suspect or a third party); and ▪ confiscation is not deemed necessary due to the nature of the particular offence. The advantages of this seizure type are as follows: ▪ little risk of damaging the equipment; ▪ little risk of harming the persons unrelated to the crime in question; ▪ little risk of interfering with activities unrelated to the crime in question; ▪ the e-evidence can be analyzed in a controlled environment. The disadvantages of this seizure type are as follows: ▪ special equipment is required at the scene; ▪ expert support is usually necessary at the scene; ▪ there is a risk of overlooking a part of the evidence; ▪ the seizure procedure is time consuming; and ▪ the relevant equipment is not put under control. **3. Seizure by confiscating the backup storage media** This type of seizure may be suitable in the similar cases as seizure by copying the entire memory contents especially if there is a very large amount of equipment and data to be considered (e.g., large networks, mainframe environments). The advantages are similar to those for a seizure by imaging described in Section 2 (there is practically no risk of damage or harmful actions). The additional advantages are that ▪ no special equipment is required at the scene; and ▪ no time consuming imaging operations need to be performed at the scene. The disadvantages of this seizure type are as follows: ▪ expert support is usually necessary at the scene; ▪ local system administrator's support is usually necessary; ▪ there is a risk of overlooking a part of the evidence (because the completeness of the backup data usually cannot be known in advance); and ▪ the relevant equipment is not put under control. **4. Seizure by selective data copying** This type of seizure should only be used under exceptional circumstances if none of the previously mentioned seizure types are possible, i.e., only selected (i.e., the most relevant) data can be copied to be analyzed later. Expert support is usually mandatory at the scene.

	The advantages and disadvantages are similar to those for a seizure by confiscating the backup storage media. A further disadvantage would be that any historical reconstruction of the computer system would be impossible. That would effectively limit their investigative value. In addition, special care must be taken to preserve the evidential value of the information seized in this way. **5. Seizure of evidence from the Internet** Seizure of evidence from the Internet is vital for many investigation types and requires specialist knowledge, skills and resources to enable it to be carried out effectively. This course will not deal with the specifics of such data collection except to reinforce that the general principles apply to this collection as to the other types that are referred to in the course. There are different types of collection from the Internet and these may broadly be broken down into the 1) collection of open source data and 2) collection by covert means. There are many legal and procedural issues that relate to this aspect and are deliberately not expanded upon. It is anticipated that this subject will be covered in an advanced module of training.
Slides 30 to 40	**E-EVIDENCE SEIZURE PROCEDURE** As mentioned in the introduction, this document focuses on the e-evidence seizure procedure involving the search for, recognition of, collection of, and documentation of electronic evidence. The procedure consists of the following phases that are described in the following sections: 1. Preparation for seizure (Section 1), 2. Securing the scene (Section 2), 3. Documenting the scene (Section 3), 4. Evidence collection (Section 4), and 5. Packaging, transport and storage (Section 5). The key principles for searching an IT environment recommended by the Council of the European Union have all been taken into consideration when developing the procedures described in the following sections. **1. Preparation for seizure** In the course of preliminary investigations aimed at obtaining a search warrant, it should be determined whether any e-evidence, which may be relevant to the case, is likely to be found. In such a case the responsible officer should inform the local data recovery unit and/or external experts as soon as possible. The first decision to be made is which type(s) of seizure should be performed (the types of seizure are described in Slide 28). As much information as possible about the IT system to be seized should be collected in advance and with expert support, such as, for example: ▪ computer hardware/operating system/software/applications and storage media related information,

- communication and network related information (ISP[4], phone, facsimile, modem, LAN[5], network equipment, etc.),
- who is responsible for the computer system and/or network (e.g., if it has a local administrator or is administered by an external company),
- how much equipment is expected to be seized (relevant to the seizure type from Section 1),
- how much data should be copied (relevant to the seizure types from Sections 2 and 4), and
- is there a system backup available on storage media (relevant to the seizure type from Section 3).

The preparation phase includes the following steps:

- Ensure that the seizure of e-evidence is correctly authorised (e.g., obtain a search warrant in accordance with applicable laws);
- Obtain as much information as possible about the IT system to be seized (see above);
- Choose the team members (incl. external experts if necessary);
- Assign individual tasks to the team members;
- Brief the team members about how to perform their tasks (they should have passed the corresponding basic training); and
- Supply the necessary seizure tools and equipment (logistics).

As mentioned earlier, all activities should be in compliance with agency policy and the EU, state, and local laws.

Seizure team members

If it is known that e-evidence might be found at the scene, the seizure team should include officers specially trained for the tasks of search and seizure of IT equipment and e-evidence. In some cases it might even be necessary to consult an independent expert (see also Section 4). For example, if the system is administered by an external company or administrator, you might consider involving him/her as an expert witness (if he/she is not considered to be a suspect). The minimum requirement is that the first responders have a basic training for collecting e-evidence.

The team members should be chosen and the tasks assigned to them by a responsible officer corresponding to the seizure procedure phases (see also the beginning of slide 30). The phases and the corresponding tasks are described in the following sections (Sections 2-5).

All team members should be adequately instructed how to perform their tasks. For example, they should know when to apply the same principles in handling e-evidence as in handling other physical evidence, and when to take some special measures (e.g., aluminium powder should not be used to collect

4 Internet Service Provider

fingerprints from electronic devices). They should also know that in certain cases they must contact an expert unit and therefore obtain this contact information in advance.

Seizure tools and equipment

Special tools and equipment may be needed to collect e-evidence. Advances in technology may dictate changes in the tools and equipment required.
The following equipment/basic toolkit set might be of value during search and seizure and should be made available by a team member responsible for logistics:

- Disassembly and removal tools:
  - Screwdrivers (flathead and crosshead, and manufacturer-specific, e.g., Compaq, Macintosh);
  - Drivers (hex-nut, star-type nut and secure-bit);
  - Pliers (standard and needle-nose);
  - Wire cutters (for removal of cable ties);
  - Small tweezers;
- Documentation:
  - Search and seizure record (property register);
  - Labels and tape (to mark and identify component parts of the system, including leads and sockets);
  - Cable tags;
  - Exhibit labels (tie-on and adhesive);
  - Other necessary forms
  - Indelible coloured marker pens (to code and identify removed items);
  - Camera and/or video camera (to photograph scene and any on-screen displays);
- Package and transport supplies:
  - Antistatic bags (for protection of equipment being removed such as circuit boards; materials that can produce static electricity such as polythene bags should be avoided);
  - Antistatic bubble wrap;
  - Cable ties (for securing cables);
  - Evidence bags and tape;
  - Boxes for packaging floppy diskettes, JAZ/ZIP-cartridges, DVDs, or CDs;
  - Packing materials (materials that can produce static electricity such as styrofoam or styrofoam peanuts should be avoided);
  - Flat pack assembly boxes or sturdy boxes of various sizes (original packaging should be used whenever available);
- Communication tools
  - Mobile phone or other communication devices for obtaining advice (should not be used in the proximity of computer equipment);
  - Contact information for assistance (e.g., phone numbers of the expert unit)

	▪ Other items: - Small torch with a bracket; - Gloves; - Hand truck; - Large rubber bands; - Magnifying glass; - Printer paper; - Seizure disk/CD (if trained to use it for forensic purposes); - Unused floppy diskettes; ▪ Transport (to and from the scene, for team members, seizure tools and equipment, and the seized evidence). **2. Securing the scene** The first responder should ensure the safety of all persons at the scene and the integrity of all evidence, both traditional and electronic. This phase includes the following steps: ▪ Follow jurisdictional policy for securing the crime scene: - Move all persons away from the immediate area from which evidence is to be collected (including equipment and power supply); ▪ Protect perishable data physically and electronically: - Identify, secure, document, and photograph each device containing perishable data; - Observe potential suspects and other persons to prevent them from altering or destroying the evidence; - Observe IT components to prevent altering or destroying the evidence. ▪ Identify and document related electronic components that will not be collected; ▪ Identify telephone and network lines attached to devices, document and label them; ▪ Decide if any other evidence is required from a device to be seized (e.g., DNA, fingerprints, drugs, accelerants); - If so, follow the general handling procedures for that evidence type laid out in the relevant handbook; - Postpone destructive techniques until after electronic evidence recovery is done; ▪ Collect latent prints after e-evidence recovery is complete (since keyboards, computer mouse, diskettes, CDs, or other components may have latent fingerprints or other physical evidence that should be preserved); ▪ Do not use aluminium powder to collect fingerprints from the scene as this may damage equipment and data. ▪ Search the scene for non-electronic but related evidence, such as: - written passwords and other handwritten notes, - blank pads of paper with indented writing, - hardware and software manuals, - calendars or diaries,

- text or graphical computer printouts,
- photographs, or
- information about personal interests that may be useful for later password /passphrase cracking (most passwords are directly related to the personal environment, such as, e.g., licence plates, partners/children, phone numbers, hobbies, etc.)

▪ Conduct preliminary interviews:
- Separate and identify all persons (witnesses, subjects, or others) at the scene and record their location at time of entry;
- Use forms/checklists or similar to collect and record information from these individuals;
- Consistent with agency policy and applicable law, obtain from these individuals information such as:
  - Purpose of the device/system (e.g., bookkeeping);
  - Owners and/or users of devices/systems found at the scene, as well as passwords (see below), user names, and Internet Service Provider;
  - Any passwords required to access the system, software, or data. (An individual may have multiple passwords, e.g., BIOS, system login, network or ISP, application files, encryption pass phrase such as for PGP, e-mail, access token, scheduler, or contact list.);
  - Any unique security schemes or destructive devices;
  - Any offsite data storage; and
  - Any documentation explaining the hardware or software installed on the system.

3. Documenting the scene

Documenting the scene is an ongoing process throughout the entire seizure procedure. It is of crucial importance to accurately document the location and condition of computers, storage media, other electronic devices, and conventional evidence. In the previous and in the following sections of Chapter 0 more detailed instructions about what should be documented are given. This section gives only a summary of these instructions.

In general, the following must be documented, but additional documentation may be created during the collection phase:

▪ Physical scene
- Draw a sketch plan of the system including, e.g., the

position of the mouse and the location of the components;
- Photograph/video/document the entire scene[6] (360 degrees of coverage, if possible);

▪ Computer systems and electronic components/devices/ equipment
- Document the following:
  - ➢ Details of all relevant equipment found, e.g., make, model, serial number;
  - ➢ Condition and location of each computer system containing or presenting e-evidence, including power status of the computer (on, off, or in sleep mode);
- Document all connections (cable or wireless) to and from the computer system or other devices;
  - ➢ Label all ports and cables (including connections to peripheral devices) to allow for exact reassembly at a later time;
  - ➢ Label unused connection ports as "unused." Identify laptop computer docking stations in an effort to identify other storage media
- Document the details of the monitor at the time of intervention.
  - ➢ Photograph the front of the computer as well as the monitor screen and other components;
  - ➢ Make written notes of what appears on the monitor screen;
  - ➢ Video active programs or create more extensive documentation of monitor screen activity.
- Document relevant electronic components that will not be collected;

▪ Information from the persons found at the scene
- Interview the persons and document their answers/complete the forms
- Document the following:
  - ➢ Details of all persons present on the premises searched;
  - ➢ Details of all persons who used the relevant computer system/equipment;
  - ➢ Remarks, comments, and information offered by the computer users/owners/witnesses.

▪ Actions taken at the scene
- Create audit trail/seizure log with the description of the action taken and the exact date and time.

4. Evidence collection

An IT system should not be seized as evidence just because it happens to be

found at the scene. Such a measure must be justified and in proportion to the corresponding offence, therefore the person who ordered the search should make a conscious decision whether an item is to be collected by the investigating authority.

Electronic evidence, as with any other evidence, must be handled carefully and in a manner that preserves its evidential value. This concerns not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of e-evidence therefore require special collection, packaging, and transportation. E-evidence that may be susceptible to damage or alteration from electromagnetic fields (such as those generated by static electricity, magnets, radio transmitters, and other devices) should be adequately protected. E-evidence should be seized according to agency guidelines and applicable laws. The following types of e-evidence will be discussed later:

- Computer system
- Other electronic devices
- Digital storage media and
- Network related information (configuration and services/applications)

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

5. Packaging, transport and storage

Computers and related devices and equipment are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, magnetic sources, and even to some actions (e.g., switching on/off). Therefore, special precautions should be taken when packaging, transporting, and storing e-evidence. To maintain the chain of custody, the packaging, transportation, and storage should be adequately recorded.

Generally, all computer components and storage media must be handled with utmost care since inexpert handling can cause damage or destruction of e-evidence.

- Packaging
  - Ensure that all collected e-evidence is properly documented and labelled before packaging.

	- Whenever possible, transport the collected e-evidence in the original package. - If no original packaging is available, use antistatic packaging (e.g., paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags. - Do not fold, bend, or scratch storage media such as diskettes, CD-ROMs, and tapes. - Do not affix adhesive labels on the surface of the storage media. Use boxes or envelopes for packaging storage media whenever possible. - Ensure that all containers holding evidence are properly labelled. - If multiple computer systems are collected, label each system so that it can be reassembled as found. ▪ Transport - Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that could damage e-evidence. - Ensure that the equipment is protected from shock and bumps (i.e., mechanical damage), heat, and humidity. - Ensure that computers and other devices that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers should be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt. - Do not put heavy objects on the smaller pieces of equipment/storage media. - Whenever possible, do not store e-evidence in vehicles for long periods of time. - Storage - Ensure that evidence is inventoried in accordance with the relevant policies. - Store evidence in a secure area, away from extreme temperature and humidity. - Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants. - Use an adequately secure store room with appropriate ➢ access control, ➢ fire protection (e.g., alarm, fire extinguishers, no smoking in the storage area or in the vicinity), ➢ temperature and humidity, and ➢ protection from magnetic sources (e.g., far from directional radio devices). - Do not store any inflammable items in the same room or in the vicinity (e.g., cleaning chemicals, or stacks of paper). - Use suitable floor covering to avoid static charges. - Do not store e-evidence in rooms with water-pipes,

	especially along the ceiling. - Be aware that potential evidence such as date, time, and system configuration may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel should be informed that a device powered by batteries (e.g., a PDA, or PC/CMOS) requires immediate attention.
Slides 42 to 51	**Investigating and analysing electronic evidence** **Computer Forensics** The term computer forensics is used to describe the systematic analysis of IT equipment with the purpose of searching for digital evidence. Forensics analysis usually takes place after the crime was committed. Compared to regular investigations, carrying out such analysis brings unique challenges as the computer technology is constantly changing and more and more information is stored in digital formats, which increases the amount of potential evidence. The focus is thereby on the ability to use the evidence in legal proceedings. This limits to a certain extent the ability to carry out forensic examinations, as they are bound by the legal standards. Even if new technical developments would enable new forensic investigations, their application is limited by the condition that those new instruments are covered by existing legal framework. **Phases of the involvement of forensic experts** Forensic experts are not only involved in criminal proceedings but also play an important role in civil proceedings, the development of protection strategies and education. With regard to criminal proceedings their involvement takes place is four phases: ▪ Identification of the relevant evidence. Forensic experts play an important role in the design of investigation strategies. They can support the law enforcement agencies in determining the best investigation technique prior to its execution. In addition to this, consultancy forensic experts can play an active role in investigation for example by analysis of the network infrastructure in the suspect's premises, in order to identify possible locations for storage devices. ▪ The preservation/seizure/collection of the evidence. The collection of digital evidence can take place at the physically location where they are stored as well as remotely. The investigators who are undertaking the first steps for the collection of evidence (first responder) have a significant responsibility for the entire investigation process. If they make poor decisions concerning the preservation of data, important traces can be lost. One example of the challenge of the task is the issue of how to handle the running computers of the suspect. Switching off the electricity supply of the computer instead of shutting it down by using commands of the

operating system is in general the suggested procedure. But in those cases where the offender was using encryption technology the disconnection of the electricity supply can lead to a decryption of files. Therefore the first responder needs to make a decision depending on the focus of the investigation.

Forensic expertise is not only relevant with regard to investigations taking place at the location where the relevant data is stored. Forensic experts can support an investigation as well by preparing a request that is submitted to service providers and assist the investigators in producing adequate case histories, which are necessary to prove the reliability of the collected evidence.

- Analysis of computer technology and digital evidence. The next phase covers all aspects related to the analysis of digital evidence as well as seized hardware. It is in general the most complex phase in the whole investigation process. The first responders often seize several storage devices. Each of the storage devices can contain thousands of files. The pure amount of data that needs to be analysed already brings great challenges for the investigators. Identifying the relevant information for the investigation and linking it is therefore one of the major tasks of forensic experts. Their work ranges from the search for illegal content in a computer system to the analysis of log-files. Not all processes undertaken by the offender while committing a cybercrime leave traces. By analysing all available evidence, forensic experts can nevertheless reconstruct the way an offence was committed. The third phase also includes the production of a full report which includes among other issues the steps of the investigation and the methods used to obtain evidence.

Examples of forensic examinations

Within the four phases (and especially within the third phase) multiple forensic examinations are possible. The choice of the right investigation technique depends on various factors – in particular, the kind of offence that is in the focus of the investigation.

Among the most common techniques are the following:

- Hardware analysis. If the investigators seize computer hardware then forensic experts can analyse the hardware to gather system-related information. Such an investigation can for example be relevant to prove whether the offender had the ability to connect a computer system to the Internet. Hardware analysis can in addition be relevant if – due to the transfer of system-related information during a registration process – it is known that the suspect used a specific hardware configuration.
- Analysis of the function of computer software. Apart from the hardware, computer software plays an important role in the operation of a computer system. Forensic experts can for example determine the functions of computer virus or other form of malicious

	software. In addition they can reconstruct software operation processes. Furthermore, software analysis can be important to determine if the production or sale of software that can be used for legitimate as well as illegal purposes (dual-use) is criminalised. ▪ Analysis of software installed on the suspect's computer system. An analysis of the software installed on a computer system can provide the investigators with valuable information for further investigation. This is especially the case with regard to encryption software and tools used to securely delete files. If such software is installed on the suspect's computer, further investigations can specifically address those issues. ▪ Identification of relevant digital information. Computer data can be stored in different types of storage devices. And even within a hard disk there are various possibilities where a file can be saved. Identifying the storage location of relevant evidence is therefore challenging. One of the new trends that presents additional challenges in identifying relevant digital information is the emerging use of remote storage. As highlighted above, the availability of broadband access and remote storage servers has influenced the way in which information is stored. By making use of such remote storage the suspect can prevent the seizure of the suspect's computer hardware enabling the law enforcement agencies to access the information that is stored on the remote storage devices. Forensic analysis can in this case be used to verify if the suspect used remote storage services. The identification of relevant digital information is not limited to files itself. Databases of software tools used by the suspect to find information on his computer might contain relevant information as well. Even system generated temporary files might contain evidence for criminal proceedings. ▪ Identification of hidden files. Offenders can use techniques to hide files in a storage device in order to prevent law enforcement agencies from analysing the content of the file. This is especially relevant within investigations concerning illegal content. Forensic investigations can identify hidden files and make them accessible within the analysis. ▪ Recovery of deleted files. If the offenders are using tools to ensure that files are securely deleting, recovery of this information is in general not possible. But in cases where the offenders are not aware of such tools, the deletion of digital information does not necessarily make them unavailable to law enforcement agencies as they can be recovered by using special forensic software tools. ▪ Decrypting encrypted files and volumes and recovery of passwords. Criminals are more and more frequently using encryption technology. This technology creates significant challenges for law enforcement agencies as they are unable to access and examine the encrypted information. Within forensic analysis, approaches to decrypt encrypted files and storage devices can be undertaken. In addition, forensic experts can support law enforcement agencies to

develop strategies to get access to encrypted files – for example, by using a key-logger.

Offenders are able not just to prevent access to certain information by using encryption, but also use password protection systems. Forensic analysis can use password recovery to enable law enforcement agencies to access password protection systems.

- File analysis. Files stored on a storage device can be analysed in various ways. Forensic examinations can for example focus on the content of files. Apart from the manual examination of suspicious files, forensic investigations can include automatic keyword searches for text files and tools that automatically search for known images on the suspect's computer.

  As highlighted previously, computer data can be rather easily manipulated. Forensic examinations can prove alterations and the forgery of digital document.

  Furthermore, investigations can take into account meta-data. These types of analyses can determine the time the document was last opened or modified. In addition, meta-data analysis can be used to identify the author of the file with a threatening message or the serial number of the camera that was use to produce child pornography image.
- Authorship analysis. If threatening texts or hate speech are posted in blogs or forums on the Internet, the analysis of log-files might not lead the investigators to the author of the text if the suspect is acting from an Internet cafe or makes use of anonymous communication services. Sophisticated linguistic analysis can help to determine if the suspect wrote articles before and left information that can help to identify the individual in this context.
- Maintaining the integrity of data. As pointed out previously, the protection of the integrity of digital evidence is crucial for the admissibility in court. Forensic experts can ensure the protection of the integrity of files during the collection of evidence. This enables law enforcement agencies in some cases to avoid the seizure of hardware and instead refer to copying the relevant files by protecting their integrity against any kind of alteration during the investigation process. This includes in particular the creation of images of storage media.
- IP tracing. Offenders that use the Internet to commit crime (for example, downloading child pornography images or attacking computer systems) leave traces. Traffic data analysis, such as the examination of log-files kept by Internet servers, can lead the investigators to the connection used by the offender to log on to the Internet. Such investigations can be challenging if the offenders use anonymous communication technology. But even in those cases investigations are not impossible. One example is the forensic tool CIPAV (Computer and Internet Protocol Address Verifier) that was used in the US to identify a suspect using anonymous communication services.
- E-mail analysis. E-mail has become a very popular form of communication and therefore plays an important role in computer

forensics. Given that it is relatively easy to identify the sender of an e-mail with threatening message or illegal content attached, offenders very often use free e-mail addresses registered using fake personal information. Even in those cases, the examination of header information and log-files of the e-mail provider can in some cases enable an identification of the suspect.

- Tracing financial transactions. A number of crimes - including the sale of child pornography – include financial transaction. By using data from commercial systems and institutions involved in the financial transactions it is possible to identify the offender. One example is an investigation in Germany where offenders who downloaded child pornography from a commercial website were identified by their credit card companies that analysed their customer records to identify customers that used their credit card to purchase child pornography on the specific website. Such investigations are more challenging if offenders make use of anonymous payment methods.
- Real time collection of traffic data and the interception of content data. Forensic investigations can include the real-time monitoring of data transfer processed. This Council of Europe Project on Cybercrime www.coe.int/cybercrime enables the investigators to react to processes at the time the suspect of an investigation is acting.
- Monitoring activities with regard to publicly available services. Publicly available services can be used to exchange copyright protected material or illegal content. Such services can within an investigation be monitored by forensic experts. This includes for example the observation of chat forums.
- Remote forensics. Currently the need for remote forensic tools is discussed. This would enable live remote evidence collection and remote monitoring, without the suspect being aware of investigations on his system.

Carrying out such investigations requires specific training and well defined procedures that are based on widely accepted standards and methodologies.

How forensic examinations are performed

There are two ways in which forensic investigations can be carried out:

- Manual operations. Despite the availability of technology to automate investigation processes, computer forensic remains up to a large degree manual work. Particularly in those investigations that involve a large amount of data, such manual operations can go along with difficulties.
- Analysis tools. Some of the processes – especially keyword searches, the reconstruction of deleted files or the decryption of encrypted material - can be automated by using sophisticated forensic analysis tools.

	Most of the investigations combine manual operations with the use of forensic software tools that automate processes. ▪ Production/Presentation of the evidence in court. In general forensic experts do not present the evidence in court, however they can play an important role in criminal proceedings. The forensic experts can be expert witnesses that help the people involved in the court proceedings to understand the processes of how the evidence was created, the procedures used to collect the evidence and the evaluation of the evidence.
Slides 52 and 59	**Part Three - Legal Issues**
	PARTICULAR QUESTIONS REGARDING THE OBTAINING OF DIGITAL EVIDENCE The modern forms of criminality on the networks, against the networks, or within the networks require the support of experts and specialized officers to gather and analyse the evidence and to do a correct interpretation of it in court. This is, of course, not new: since many centuries experts help judges, prosecutors and lawyers to understand technical questions. For example, for many centuries, doctors have been essential to determine, clarify and evaluate in court the probable cause of a murder in medical terms. But the is that the digital environment brings new and different questions, still difficult to solve. In fact, the permanent technical development is not always followed by a continuous revision and update of the legal instruments and not always procedural legal tools legitimate the raising techniques of gathering electronic evidence. On the other hand, normally, initial and continuous training of both law enforcement agents, prosecutors and judges, don't follow the technical evolution without delay. In this scenario, there is an increasing introduction of new criminal infringements, whose understanding depends on special knowledge. Technical expertise is not just needed to prove criminal activity; it is needed to understand what exactly the crime in question is. While we all understand what "murder" means, and need medical experts only to establish the cause of death, "Denial of service" is a crime that is defined by a certain technical understanding of computer networks. Around the world, most of the countries don't have specific regulation on electronic evidence. Some of them have special rules respecting, for example interception of communications. But in general, legal systems based gathering of electronic evidence on the pre-existing rules, already applicable

	to the offline world. In some cases, courts accept the new evidentiary realities, adapting themselves the classical rules; in other cases, they don't. In these kinds of situations, new provisions must be added to the existing legal framework. Many European countries did not yet introduce legislation concerning electronic evidence and the criteria that courts should use examining and evaluating electronic evidence. Gathering and evaluating electronic evidence is a delicate activity, because normally touches fundamental rights, such as privacy or the secrecy of telecommunications. And, sometimes, it is not clear to the judge if those rights are respected. Cybercrime is global. The criminal facts can occur simultaneously in more than on country and jurisdiction. By its nature, cybercrime is transnational. Crimes committed within the information and communication networks created serious problems to clarify the place where the infringement took place, and the competent law enforcement authority to carry out the case. The Budapest Convention on Cybercrime could not solve all the problems related to this, but tried to find solutions for some difficult situations. The Parties to the Convention, as usually in other cases, will investigate the crimes committed on its territory. But the Convention states, in addition, that the Parties should declare themselves competent to prosecute and try cases involving their own citizens when the crime was committed abroad, provided that the activity in question was also punishable under the local law where the action took place. This is an important practical issue. Although some countries have provisions defining their universal jurisdiction, it is not a generally or universally recognised principle. However, in many situations it can be difficult to clarify which court has jurisdiction according to the general rules. For instance, a computer offence can perfectly be committed simultaneously in several countries over several victims, or can be committed by different authors, from different locations. Since criminal jurisdiction rules are not harmonised in all the countries, it might well happen that two courts, located in different countries, claim jurisdiction over one single offence, despite the general rules contained in the Convention on Cybercrime. At the European Union level, it was issued an important Directive, respecting exclusively to the gathering of digital evidence: Directive 2006/24/EC, of the European Parliament and of the Council, of 15 March 2006 was the first binding document within the European Union on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

	Practical Exercises (if applicable) No practical exercises are envisaged for this particular session as there is no guarantee that the level of technology and Internet access to deliver such exercises will be available at all venues. Trainers may in the future seek to supplement to learning by adding exercises, where the training is delivered in an environment where the facilities are suitable.
	Knowledge Check No specific knowledge check in addition to that listed above is currently envisaged for this course. No official assessment has been requested
Slide 63 to 64	**Summary / Recap** The trainer should recap / test knowledge on the following objectives to ensure they have been met during the session: ▪ Discuss various types of electronic evidence ▪ Explain the principles of best practice relating to the seizure and handling of electronic evidence ▪ Identify the challenges offered by "dead box", "live data" and Internet sources of electronic evidence ▪ Identify the challenges of obtaining evidence from another jurisdiction ▪ Discuss the issues of admissibility of electronic evidence in judicial proceedings, in terms of its authenticity, accuracy, completeness This may be achieved by way of group discussion, questioning of the participants, a quiz or other recognised methods. This lesson has sought to provide some guidance as to the type and level of knowledge of electronic evidence that is required by Judges and prosecutors to fulfil their role effectively. It does not purport to be a complete analysis of the issues and where relevant indicates where further information may be obtained. It is recommended that training developers ensure that the material they prepare is as up to date and incorporates the latest issues as they impact on criminal behaviour; its impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered. There are technological changes that will affect the criminal justice system, such as solid state storage of data and Web 2.0. These will be important issues to include in training programmes and require inclusion as they become more prevalent.

6.9 Lesson 1.3.4 International Cooperation	Duration: 90 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation

Aim:

This session wants to recall the importance of international cooperation and present an overview of the available instruments for international cooperation in the field of cybercrime, mainly the Budapest Convention on Cybercrime – it will be an introduction to the available instruments, the ways they are used, the timelines and the effectiveness.

Objectives

By the end of the session, delegates will be able to:

- Recognize the global dimension of Internet and the international dimension of cybercrime
- Explain the importance of international cooperation and recognise the available instruments for international cooperation in the field of cybercrime
- Identify the need of very fast and efficient channels for international cooperation and the available instruments, the ways they are used, the timelines and effectiveness
- Describe the efforts from international organisations regarding the implementation of new modalities of international cooperation
- Discuss the Budapest Convention on Cybercrime - identify its general principles, the provisional measures and the 24/7 network on mutual legal assistance

Slides nr.	Content:
	Introduction This session will underline the importance of international cooperation to the investigation of concrete cases of cybercrimes. International cooperation available instruments, mainly the Budapest Convention on Cybercrime, will be described.
Slide 2	1. Part One of the presentation will focus on the international dimension of cybercrime. As this topic was already referred in other sessions, this will be a very brief approach. 2. On Part Two will list some responses to cybercrime at the international level. 3. Part Three, regarding the international response to cybercrime, will underline the role of the Budapest Convention on Cybercrime. 4. Finally, Part Four will focus on the international cooperation tools described in the Budapest Convention. 5. Part Five will recover the major topics of all the presentation.

Slide 3	**Session Objectives** The purpose of this session is, generally, to recognize the global dimension of the Internet and the international or transnational dimension of cybercrime. International cooperation and the available instruments for international cooperation in the field of cybercrime will be referred to. The need of very fast and efficient channels for international cooperation will be underlined in addition to providing a description of the available instruments for such cooperation. Provide an overview of the efforts from international organisations regarding the implementation of new modalities of international cooperation. In particular, there will be reference to the Budapest Convention on Cybercrime – by identifying its general principles, the provisional measures and the 24/7 network on mutual legal assistance.
Slide 4	**Part One - The international dimension of cybercrime** In a very brief approach the international dimension of cybercrime will be revisited.
Slide 5	It is an obvious fact that Internet is globally expanded and can be accessed and used by almost everybody in the planet. Within the networks, crime is raising. And consequently, cybercrime must be approached as a global phenomenon. The full reality of cybercrime cannot be understood without recognising the international dimension.
Slide 6	In this context, cybercrime is the most transnational of all crimes. And those who want to investigate cybercrime must be aware that their task requires efficient international cooperation. In fact, being global by its nature, without international cooperation, cybercrime investigations are unlikely to succeed.
Slide 7	In concrete terms, when a crime is committed in cyberspace, criminal justice authorities face very difficult questions that they must solve before anything else. Considering that the Internet is everywhere, it is not always easy to determine the legally relevant location of the crime. If, for example, the perpetrator acts in place A and the targeted victim computer is in place B, but the illegal communication used by the criminal was carried by a provider based in place C, and if all those locations belong to different jurisdictions, the first question that the law enforcement official must solve is the legally relevant location of the crime, in terms of jurisdiction. It must be clear which is the place where the crime was committed, so that it can be determined which is the applicable substantive law and which is the competent jurisdiction (police, prosecutor, judge).

	The investigator must respect its own jurisdiction – its own territorial competence. According to this point of view, jurisdiction will be a binding limit to criminal investigations. This reality raises two kinds of unsolved questions. ▪ The first one regards cross border investigations: how can lawfully a law enforcement agent investigate outside his own country, if he needs to act urgently? How can he obtain and gather evidence stored "next door", in another country if he feels that the evidence can very quickly disappear? ▪ The second question regards investigation in the "cloud". No one knows where (physically) can be stored some data, supposedly it is stored in the "cloud". It is possible that none knows what can be the national jurisdiction on some data, in the "cloud". How can a law enforcement agent obtain and gather data stored in the "cloud", wherever it is physically stored?
Slides 9 and 10	**Part Two - International response to cybercrime** As Internet has globally expanded and is used nowadays by potentially everybody in the planet, cybercrime must be approached as a global phenomenon. The purpose of Part Two is to describe some of the most important steps given to respond to cybercrime, in a practical approach, within Europe.
Slides 11 to 13	Interpol is a very well known international organisation, whose members are law enforcement bodies from all over the world. Interpol counts, by January 2012, 190 members from all continents. Its objective is to enhance and facilitate international police cooperation. For that purpose, Interpol organised a global police communication system and developed specific databases and police information analyses. Interpol was one of the first international institutions to show concern on cybercrime issues, and one of the first to organise discussion groups of experts on the topic, in 1995. Since then, Interpol developed efforts to help police and other law enforcement agencies around the world to strengthen their ability to combat cybercrime. To achieve that goal, Interpol built a contact point network (Interpol National Central Reference Points - NCRP), which seeks to provide assistance to its members on a permanent basis. NCRP had, by September 2011, around 120 reference points all over the world. These reference points adopted the layout of the 24/7 contact points created by Article 35 of Budapest Convention on Cybercrime. In some of the countries that are Parties to the Convention, the Interpol reference point was also appointed as the G8 contact point. All the G8 contact points were included into this network. The objective of this structure was to enable police to immediately identify experts in other countries and obtain immediate assistance in computer-related investigations and evidence collection. This network is

	available 24 hours per day, seven days a week. NCRP's scope is to provide exchange of police information and intelligence between its members and to provide technical and operational support. In fact, the main purpose of NCRP is to ensure that the typical police information can be exchanged as quickly as possible, through specific and appropriate Interpol channels; this includes information on suspected terrorists, wanted persons, fingerprints, DNA profiles, lost or stolen travel documents, stolen motor vehicles, stolen works of art, etc. This type of potentially important information provided by Interpol is surely very useful to concrete investigations. However, precisely because of the scope of the network, it cannot be used to urgently request, for instance, of preservation of computer data, or preservation of traffic data, or any kind of measure in order to obtain or conserve evidence. In other words, the kind of cooperation that can be provided by this specific Interpol network is based on the same principles that are otherwise applied to the general Interpol cooperation.
Slide 14	The European Union is a supporter of the Budapest Convention – even participated, as observer, in the drafting of the Convention. Since then, the European Union encouraged all Member States to ratify the Convention. In fact, a large number of Member States ratified it and all of them already signed. Of course, within the Union, a wide range of international cooperation tools are available, even outside the most recent approaches, based on the principle of mutual recognition. Most of the advantages of the European system are based in the possibility of direct contacts between judicial authorities from each Member State. According to this possibility, each judge or prosecutor can directly present a request to another judge or prosecutor. This is a very strong tool respecting investigation, also suitable on cybercrime matters.
Slide 15	In addition, in 2005, the European Union adopted a binding instrument concerning, among others, a 24/7 contact point network, regarding cybercrime investigations - the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. This framework Decision includes, in particular, rules referring to the "existing contact points network" - Article 11, 1, states that all European Union Member States shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. This is a provision respecting exchange of information relating to some listed offences (illegal access to information systems, illegal system interference, illegal data interference and instigation, aiding and abetting and attempt referred to the other). It is not said in the articles of the framework decision, but it is clear that the *existing network* is the G8/Council of Europe network.
Slide 16	Europol is an autonomous organisation of the European Union the aim of which is to improve the effectiveness of co-operation between law

	enforcement authorities from each European Union Member State. Its activities, since 1999, include facilitating the analysis of criminal information and sharing of data between Member States. Cybercrime is one of the most important areas of activity of Europol. Among many other possibilities, Europol can be an excellent channel to increase the efficiency of the provisions of Article 26 of Budapest Convention, respecting spontaneous information. In January 2013, the European Cybercrime Centre (EC3) was established at Europol.
Slide 17	No one knows where Eurojust will arrive in the future, but currently it is already an important European Union agency, dedicating to the judicial (prosecution and judicial level) cooperation, among member States of the European Union. The scope of Eurojust is international cooperation in the fight against important crime, by the means of coordination of the activities carried out by the national authorities responsible for prosecution. In this context, Eurojust has competence to promote coordination between the competent authorities of the various Member States and to facilitate the implementation of international mutual legal assistance and of extradition requests. Eurojust was created, with legal personality, in December 2000, after the recommendation made by the Tampere European Council and gathers one representative from each one of the 27 Member States. "Computer crime" is one of the areas of competence of Eurojust.
Slide 18	Still with the aim of fighting against organised crime and terrorism in the European Union, by the way of increasing and simplifying the cooperation among judicial authorities, the European Judicial Network in Criminal Matters was established, within the European Union, in June 1998. It is, in fact, a network of judicial contact points, based on the central authorities in each Member State responsible for international judicial cooperation, national contact points, in each Member State, and eventually liaison magistrates. One of the scopes of the European Judicial Network in Criminal Matters is to provide background information, available to magistrates, to make easier international cooperation between different judicial organizations and legal orders. In this context, the European Judicial Network in Criminal Matters developed the Atlas, a computer tool which allows practitioners to easily identify the competent local authority in each Member State to receive and execute a mutual legal assistance request. It is supposed that the contact points are available to be contacted by local judicial authorities to facilitate judicial cooperation between the Member States and to also support those authorities to prepare requests for judicial cooperation. Such kind of a network

	k, which provides for very fast and easy submission of requests for cross-border cooperation, can be very valuable in gathering electronic evidence.
Slide 19	European Convention on Mutual Assistance in Criminal Matters of the Council of Europe, from 1959, is the obvious background to Budapest Convention on Cybercrime. In fact, Budapest Convention does not want to cover all the existing issues on international cooperation; the text just refers to new and previously non-existing, or faster, channels and modalities of cooperation. All the Member States of the Council of Europe (with the exception of San Marino) ratified this Convention, what means that, from all the Parties of Budapest Convention, the only non-member Party of the Convention of 1959 are the United States of America. This fact attests to the added value of the Budapest Convention in creating, for the first time, a common legal framework for international police and judicial cooperation between most European States and the United States. This is a particularly important aspect because Article 14, 2, states that the procedures on international cooperation of the Convention shall apply, in addition to the criminal offences established in accordance with Articles 2 through 11 of the Convention, as well as to other criminal offences committed by means of a computer system and to the collection of evidence in electronic form of any other criminal offence.
Slide 21	**Part Three - International response to cybercrime: Budapest Convention on Cybercrime**
Slides 22 to 25	As it was already mentioned in other lessons, Budapest Convention was opened for signature on 23 November 2001 and entered in force in July 2004. By April 2013, 57 States were either Parties, signatories or have been invited to accede. In concrete cases of investigations on cybercrime matters, the Parties of the Convention gain the possibility to use, mainly when international cooperation is required, new and very innovative tools of investigation. These new possibilities can be used when the crime under investigation is one of the offences described in the Convention, but also in other cases, if the crime was committed by the means of a computer system or the evidence of the crime is recorded or stored in digital means. That is stated by Article 14 of the Convention. It was the first time that the international community made concerted efforts to agree on a universal treaty on matters relating to cybercrime and electronic evidence, with the hope that eventually most States would rally behind its purpose. Today, it remains the first and only binding international instrument on cybercrime. Each country that ratifies the Convention and becomes a Party gains in the process very relevant access to a universal *forum* of co-operation, both with

	police forces and with judicial bodies. The Convention introduces new channels for international cooperation. Some of its provisions are highly innovative and exceptional, but can be considered as adequate and necessary responses for the new realities of cyber criminality. Nevertheless, the Convention on Cybercrime does not seek to be the only binding international instrument on international cooperation. It is assumed by the Convention, in Article 23, that the Convention itself will be applicable in the framework of other existing relevant instruments on international cooperation in criminal matters. Consequently, Article 27 describes the general principles that should be observed in the absence of applicable international conventions or treaties. On the other hand, it must be underlined that the rules introduced by the articles of the Convention create new cooperation tools and channels between the Parties that were not allowed by any previous instrument.
Slide 27	**Part Four - Budapest Convention - international cooperation tools** The rules of the Convention, with respect to international cooperation, are described under chapter III of the Convention. Most of the rules under this chapter are operational and procedural rules, also common to other international conventions. Others are much innovative and must be explored in more detail.
Slides 28 and 29	Article 26 describes the situation that occurs when the authorities from a Party, during a national investigation, discover that some of the information they obtained should be forwarded to the authorities of another Party – but without having received a request from this state. This can be done if the information seems to be useful or necessary to initiate an investigation with respect to a criminal offence in the framework of the Convention. While in the past mutual assistance was typically passive, state A requesting assistance from state B, the Convention encourages a more proactive approach. However, this "spontaneous" supply of information, according to of Article 26 point 2, can be made subject to certain conditions, as for example requesting of confidentiality or a specific use of the data.
Slides 30 to 32	Article 29 is one of the most important provisions of Budapest Convention. Article 29 defines rules regarding the expedited preservation of data stored in a computer system. It establishes a parallel framework to the domestic provision regarding expedited preservation of data. In general, this provision allows a contracting Party to require from another Party the expedited preservation of data, if at the same time it expresses its intention of doing a formal request of assistance for a search, or a seizure, or any similar measure. In this case, the requested party must act as necessary, with all the due diligence, to preserve the requested data, according to its own national law. As it was already mentioned, this is a new tool of international cooperation.

	This new tool is the result of the specificity of the digital environment. Cross border assistance is notoriously time consuming. The expedited character of the measure is a need imposed by the necessity to preserve something that, in very short moments, can be completely deleted. It is relevant to point out that this is only a preservation measure, for urgent reasons and does not imply automatically disclosure of the preserved data. In fact, in the cases where disclosure is permitted, there are very narrow rules which allow it, above all if the data are not merely traffic data. In practical terms, an expedited preservation of data can be carried out and then, later on, it may turn out that there are reasons not to disclose this data to the requesting party. It is important to consider, that dual criminality cannot be required by the requested party, as a condition of preservation of the data.
Slides 33 and 34	Disclosure of traffic data is described under Article 30 of Budapest Convention. With respect to traffic data, the text of the Convention proscribes an easier model to facilitate international cooperation. There are no specific rules to expedited disclosure, as there are no specific rules to expedited disclosure at the domestic level, in the chapter of procedural rules. Indeed, without explicitly saying so, the Convention harmonises domestic rules of expedited evidence preservation and disclosure and those governing international cooperation.
Slides 35 and 36	Article 31 of the Convention defines a general rule on the mutual assistance regarding accessing of stored computer data. While this article, and Article 23 to which it refers, express a general aspiration that parties will collaborate in the prosecution of cybercrime in the "widest possible extend", it does not create new cooperation duties. All cooperation is subject to the existing treaties and international instruments that regulate cross border cooperation in traditional investigations. In practical terms, Article 31 just brings to the cyber environment general rules, already applicable in the real life, for years.
Slides 37 and 38	Article 32 defines the possibility given to law enforcement agencies from a Party State of the Convention, to obtain evidence stored in a computer physically located in another Party's territory, without any request of international cooperation. This can be done if, during a concrete investigation, the officers in charge need to obtain open source information from a computer located in a foreign country or from a computer which access was authorized by the lawfully authorized person. Regarding open source information, it must be noted that this "open source" investigation is something that any citizen can do, by his own initiative, in most countries. This provision thus simply aims to authorize law enforcement agents to do it as well and, at the same time, qualify as valid the evidence obtained in such a way. But the other side of the provision has a very new approach. There is no

	real equivalent in the physical world to this new possibility: in the past, an officer would have to travel physically to the other country and ask for assistance of the local authorities. He could not do anything by his own and every investigative act would be practised on behalf of the national authorities of the location. Article 32 states the opposite. According to it, any law enforcement agent from any country in the whole world can obtain information from another country, even if it is "not open source" information, if the person who has the lawful authority to disclose the data gives his or her lawful and voluntary consent. That investigative activity does not need any authorization of the State with jurisdiction in the place where the information is stored. Some States don't accept peaceful the Convention because of this drafting. They claim it goes against the principle of sovereignty. However, there is not any proposal or any other solution to the complex problems of cross-border investigations or to investigations in the "cloud". The real life reveals that, in most cases, it is impossible to investigate cybercrime or gather electronic evidence, at the international level, using the traditional channels. It is impossible because the time it takes is not compatible with the volatility and fragility of electronic evidence. That is why a cross-border investigation, conducted by the law enforcement agent who is dealing with the case would be more efficient. But, on the other hand, sometimes it is really impossible, at all, to use the regular cooperation channels – regarding services in the "cloud", the users (and the investigator) don't know exactly where the data required by the police, physically, are stored.
Slides 39 and 40	Article 33 regards international cooperation on interception of communications. This is not a new international cooperation tool: other international binding instruments refer to it. However, Article 33 has a specific scope: the real-time collection of traffic data. On the other hand, the most important rule stated in Article 33 refers to the limits of the application of this investigative measure. And the limits are the conditions and procedures provided for under domestic law. Thus, this modality of cooperation will be provided by each State in the same cases for which real-time collection of traffic data would be available in a similar domestic case.
Slides 41 to 43	Article 35 is one of the most important operational provisions of the Convention. Article 35 imposes to all contracting Parties the obligation to create a permanently available contact point (a so called 24/7 network of contact points). The general objective of these contact points is to facilitate international co-operation. They can do that by giving technical advice to other contact points, activating the proper mechanism to expedited preservation of data, urgently collecting evidence, or identifying and discovering suspects.

	This operational network of experts on high-tech criminality was designed to assist other experts, from other countries or jurisdictions, in criminal investigations with international connexions. It wants to face the new challenges caused by the new speedy high-tech criminalities. Sometimes, computer crime investigations need to preserve, in a very fast way, electronic data, so as it can be possible locate and prosecute suspects. This new need cannot be satisfied by any traditional channel of international cooperation. That is the added value of this network: it can provide help and cooperation very quickly even if a formal cooperation request must follow this informal way.
	Practical Exercises (if applicable) No practical exercises are prepared for this session
	Knowledge Check The trainer should check knowledge by asking relevant questions from each of the session aspects.
Slides 45 and 46	**Summary / Recap** The trainer should recap / test knowledge on the following points: ▪ Recognize the global dimension of Internet and the international dimension of cybercrime ▪ Explain the importance of international cooperation and recognise the available instruments for international cooperation in the field of cybercrime ▪ Identify the need of very fast and efficient channels for international cooperation and the available instruments, the ways they are used, the timelines and effectiveness ▪ Describe the efforts from international organisations regarding the implementation of new modalities of international cooperation ▪ Discuss the Budapest Convention on Cybercrime - identify its general principles, the provisional measures and the 24/7 network on mutual legal assistance

6.10 Lesson 1.3.5 Course Closure	Duration 90 Minutes

Resources required:

- Laptop or PC running Windows 7 and with Office 2010
- Projector
- PowerPoint Presentation
- Delegate evaluation forms

Aim:

This session is designed to allow the delegates to provide feedback on the course and to assist the trainer in identifying any improvements that may be made. It is also for the trainer to recap on the contents of the course by reference to the aim and objectives.

Objectives:

At the end of this session participants will be able to:

- Provide appropriate feedback on the course and its effectiveness
- Complete the COE course evaluation forms
- Identify the next level of learning that they need to undertake to improve their knowledge and skills in the subject matter.

Introduction

This is an important session of the course and should be used to obtain feedback from the students on the course content and methodology used to deliver the course. Any evaluation forms should be completed or finalised during this session. The trainer should recap on all the session of the course and check that the objectives have been met. Once the session is over the trainer is responsible for ensuring that all feedback in considered and that any changes that are necessary, are implemented in the course either as an ongoing minor modification or during a scheduled major modification update.

Slides nr.	Content:
Slide 1	**PowerPoint** (or other type of presentation) A PowerPoint is provided to assist the trainer in encouraging discussion about all of the sessions of the course. The trainer should hand out the evaluation forms before commencing this session. In some circumstances, it may be appropriate to issue the evaluation forms at the beginning of the course in order that delegates may complete them as the course progresses and when the sessions are fresh in their minds. There is also a tendency at the end of the course for people not to complete them fully.
Slides 2 and 3	As with all previous lessons this should follow a similar form with the agenda and session objectives set out at the beginning of the lesson.
Slides 4 to 21	The timetable is a useful way of reminding the delegates of the content of the course and is included to assist the trainer The trainer should recap the agenda and session objectives for each of the sessions. Feedback and suggestions from the delegates should be noted for future use.

Slide 22	It is the trainer's responsibility to ensure that the delegates complete the evaluation forms. The trainer should collect the completed forms and hand them to the COE representative at the course or return them to the COE at the earliest opportunity.
	Practical Exercises (if applicable) Other than completion of the COE evaluation form, there are no practical exercises associated with this session
	Knowledge Check The session lends itself to the trainer being able to check the knowledge gained by students by asking questions during the feedback stage.
	Summary / Recap The trainers should ensure that adequate opportunities have been provided for the students to give feedback and that the feedback is collected.

7 Evaluation

Evaluation is an important part of a training course and should be accorded the time it requires for delegates to provide considered feedback on their learning experience.

This course has been developed as a generic course and as such much of the teaching materials are PowerPoint based and without the level of practical exercises that may normally be associated with this type of course.

An evaluation form has been prepared and follows in this section. Trainers are responsible for ensuring that the forms are completed and returned to the Council of Europe in order that improvements may be made for further deliveries of the course.

8 Assessment

No assessment has been requested for this course, however, those delivering the materials in the future, especially those in countries where the course may be part of a programme that is assessed may reconsider this. If assessment is introduced, the methodologies in that country should be used.

Appendix

Training materials and students materials