



www.coe.int/cybercrime

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

Version 1.0 - December 2020

Specialised Course on Electronic Evidence for Judges and Prosecutors

Trainer manual

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contact:

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

Tel: +33-3-9021-4506

Fax: +33-3-9021-5650

Email: alexander.seger@coe.int

Disclaimer:

This technical report does not
necessarily reflect official positions of
the Council of Europe or of the donor
funding this project

Table of content

1	INTRODUCTION	4
1.1	HOW TO USE THIS TRAINER MANUAL	4
1.2	COURSE BACKGROUND	4
1.3	OBJECTIVES	5
1.4	TARGET AUDIENCE.....	6
1.5	TRAINER REQUIREMENTS	6
1.6	COURSE AND HARDWARE REQUIREMENTS	6
1.7	COURSE TIMETABLE	7
2	SCENARIO.....	8
2.1	INTRODUCTION OF THE SCENARIO.....	8
2.2	THE HOUSE SEARCH.....	10
2.2.1	THE LIVING	10
2.2.2	BEDROOM 1.....	11
2.2.3	BEDROOM 2.....	12
2.2.4	BEDROOM 3.....	13
3	LESSON PLANS.....	14
3.1	LESSON: 0 – COURSE OPENING	14
3.2	LESSON: 1 – INTRODUCTION TO ELECTRONIC EVIDENCE.....	15
3.3	LESSON: 2 – REFRESHER COURSE ON THE CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION).....	16
3.4	LESSON: 3 – CIVIL LIBERTIES AND SAFEGUARDS WITH RESPECT TO ELECTRONIC EVIDENCE.....	18
3.5	LESSON: 4 - DEVICES, NETWORKS AND DATA.....	20
3.6	LESSON: 5 – AUTHORISATION TO COLLECT ELECTRONIC EVIDENCE.....	21
3.7	LESSON: 6 – COLLECTION OF ELECTRONIC EVIDENCE	23
3.8	LESSON: 7 – VIDEO	25
3.9	LESSON: 8 – PRACTICAL EXERCISE (PHASE 1 – COLLECTION OF ELECTRONIC EVIDENCE).....	26
3.10	LESSON: 9 – PRACTICAL EXERCISE (PHASE 2 – ASSESSMENT OF ELECTRONIC EVIDENCE).....	28
3.11	LESSON: 10 – EXAMINATION AND ANALYSIS OF ELECTRONIC EVIDENCE	29
3.12	LESSON: 11 – PREPARATION OF ELECTRONIC EVIDENCE FOR COURT	31
3.13	LESSON: 12 – ADMISSIBILITY OF ELECTRONIC EVIDENCE.....	32
3.14	LESSON: 13 – PREPARATION FOR EVIDENTIARY HEARING	36
3.15	SESSION 14: PRACTICAL EXERCISE (PHASE 3 - EVIDENTIARY HEARING + PHASE 4 - JUDGEMENT).....	38

1 Introduction

Welcome to the specialised training course “Electronic Evidence for Judges and Prosecutors”. This course covers the broader overlapping rules and principles about evidence collection, preservation, analysis, preparation and admissibility that are similar across both civil law and common law jurisdictions.

The course is designed as a 4-day training course delivered in a physical classroom setting. While the first one and a half days concentrate on knowledge delivery by the trainer, the rest of the course requires the participants to work on a case scenario. This scenario at the core of the training involves a case file, video clips, reports, warrants and statements on the collection and examination of electronic evidence. The participants will be required to assess all evidence and its admissibility from the different angles of parties in the criminal justice system. By the end of the training, all evidence will go through an evidential hearing and judgement.

1.1 How to use this trainer manual

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.

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. These will be important issues to include in training programmes and require inclusion as changes become more prevalent.

This trainer manual is made of the following three chapters:

1. The introduction chapter helps setting the frame for the training by explaining the background, objectives, target audience, prerequisites and the timetable for the course. This will help the trainer in assessing the scope of the training, choosing the appropriate participants and preparing the classroom for the delivery.
2. The scenario chapter will guide the trainer through the scenario which has been developed for this course. The scenario is at the core of the training and should be studied carefully by the trainer.
3. The lesson plans chapter will give more in-depth details for each session in the timetable. Each lesson plan includes a list of resources required to deliver that session as well as the aims, objectives and useful information for the delivery of theoretical and practical contents.

1.2 Course background

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.

In this context, training materials such as the basic and advanced “Cybercrime and Electronic Evidence Training Courses for Judges and Prosecutors” have been developed and updated by the Council of Europe since 2012. The basic and advanced courses have been successfully delivered to a large variety of countries worldwide through different projects, such as CyberCrime@IPA, CyberCrime@EAP, CyberEast, CyberSouth, GLACY (+) and iProceeds (2). Moreover, the course contents were not just taught in the countries but were flanked by “Training of Trainers Programme” and the course materials were provided to training institutions in countries. This approach follows the objective of enabling training institutes in countries to deliver initial and in-service cybercrime training on a long term, sustainable basis.

Building up on that approach this new specialised course has been created to focus specifically on the technical nature of electronic evidence, its evidential value, the digital crime scene, the virtual investigative biotope and how to deal with that practically and legally. Similar to the “Advanced Cybercrime and Electronic Evidence Training Courses for Judges and Prosecutors” this course designed around a practical case scenario. This time however the scenario focusses on the admissibility of electronic evidence in an evidential hearing and the evidence will be assessed, challenged and defended by the participants who need to take the perspectives from the different parties involved in such a hearing.

1.3 Objectives

The objective of this specialized course is to focus specifically on the technical nature of electronic evidence, the digital crime scene, the virtual investigative biotope and how to deal with that practically and legally. Lawyers generally do not have a technical background but are called upon to deal legally with a technically challenging investigative environment in which evidence is gathered. It should not be a goal to turn law practitioners into IT- experts, but they should be brought to a basic and minimum understanding of how some technical procedures work in order to make the right decisions, to issue the right warrants and to render the right judgement.

1.4 Target audience

This training course is designed as a 4-day training programme for judges and prosecutors as part of their initial training programme or in-service programme where they have not had the earlier benefit of this training.

1.5 Trainer requirements

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. For this course it is particularly important to include trainers that have some experience of this type of investigation and trial hearings. To this end it may be appropriate to utilise the knowledge and skills of those from the law enforcement cybercrime community.

1.6 Course and hardware requirements

For the implementation of this course, in addition to a plenary classroom, there is also a need for break- out rooms, where the various teams can deliberate and work. If the plenary class is large enough, it is also possible to work with 'islands' in the same room.

It is advisable for participants to bring their computers with them. The intention is to make the exercises paperless. Also for this reason, the participants need to have a laptop or tablet.

It would be appropriate that every group could have a beamer and screen at their disposal in order to facilitate the group work and the collective drafting of documents (motions, statements, judgement...). The groups are encouraged to use PowerPoint to support their (written) statements and arguments in court. Depending of the setup and preference, the student groups should have access to whiteboards, flipcharts and notepaper including appropriate pens.

1.7 Course timetable

	09:00-09:30	09:30-10:00	10:00-10:30	10:30-11:00	11:00-11:30	11:30-12:00	12:00-12:30	12:30-13:30	13:00-14:00	14:00-14:30	14:30-15:00	15:00-15:30	15:30-16:00	16:00-16:30	16:30-17:00	
Day 1	Course Opening and Introductions 30 minutes	Session 1 Introduction to Electronic Evidence 1 hr	Session 2 Refresher course on the Budapest Convention 2 hrs					BREAK	Session 2 (cont.) Refresher course on the Budapest Convention 1.5 hrs			Session 3 Civil Liberties and Safeguards 45 minutes		Session 4 Devices, Networks and Data 1 hr		
Day 2	Session 4 (cont.) Devices, Networks and Data 2,5 hrs					Session 5 Authorisation to collect electronic evidence 45 minutes		BREAK	Session 6 Collection of Electronic Evidence 2,5 hrs					Session 7 Video Scenario 20 minutes	Session 8 Practical exercise Phase 1 30 minutes	
Day 3	Session 9 Practical exercise - Phase 2 2 hrs				Session 10 Examination and analysis of electronic evidence 1,5 hrs			BREAK	Session 10 (cont.) 0,5 hrs	Session 11 Preparation of electronic evidence 45 minutes		Session 12 Admissibility of electronic evidence 2 hrs				
Day 4	Session 13 Preparation for evidential hearing 2 hrs				Session 14 Practical Exercise Phase 3 - Evidentiary Hearing 1,5 hrs			BREAK	Session 14 (cont.) Practical Exercise Phase 4 - Judgement 0,5 hrs	Course closure						

2 Scenario

As explained in chapter 1 this training is heavily based on a scenario which involves the participants, will lead to interesting discussions and will finally be judged after an evidential hearing.

Knowledge about this scenario is essential for the trainer. Please read this chapter carefully. You will find a more detailed version of the scenario including all the evidential items, reports, etc in a digital “case file” in the folder of “Session 9”.

2.1 Introduction of the scenario

Today is **2029-04-10** and you are about to take part in an ongoing investigation.

What preceded:

There has been a mass shooting in a mosque in New-Zealand, with more than 50 casualties as a result. The attack was performed by a white supremacist who wanted to hit hard on the Muslim community.

From intelligence services you receive information that a person in your country could be identified as a suspect who made a video which was distributed via the Telegram¹ channel *@pinkbird* (an IS linked channel). In this video he announces a plan to retaliate on behalf of IS/Daesh with a suicide attack in a public place somewhere in your country.

The video shows images of an AK47 assault rifle and a bomb belt which seems to be professionally put together. Open Source Intelligence (OSINT) investigation could not determine if the images of AK47 and the bomb belt are recuperated from already existing images on the internet. The Telegram profile of the suspect could be linked to a mobile phone number +1 (415) 555-2671 in the database of Interpol which was previously detected in a Spanish counter-terrorism (CT) investigation. Telecommunication investigation shows that the prepaid number is no longer activated (out of use since 12 September 2028 and no identification possible).

The suspect presumably could be identified as the named **Sam**, 22 years old, last known to be living in your capital. Currently he is under the radar, without a fixed address. Through OSINT he can be linked to a Facebook (FB) profile named ‘Paradise lost’, on which he posted three months ago a picture of himself, with his index finger raised, with reference to the Shahada². No other recent FB activity is detected. The EXIF³ data of the picture could be interesting since the picture looks to be taken in a living room somewhere. As there has been no activity on the Facebook profile for over three months, there are no recent Facebook log data available. Facebook lets you know that EXIF data are indeed gathered by Facebook when someone uploads a picture but that the retention period of those data is very short (approximately 7 days).

¹ Telegram is a cloud-based instant messaging, videotelephony and voice over IP service. [Wikipedia.org]

² The Shahada, also spelled Shahadah, is an Islamic creed, one of the Five Pillars of Islam and part of the Adhan, declaring belief in the oneness (tawhid) of God and the acceptance of Muhammad as God's messenger, as well as the wilayat of Ali according to Shia Islam. [Wikipedia.org]

³ Exif is a format for storing metadata in image and audio files

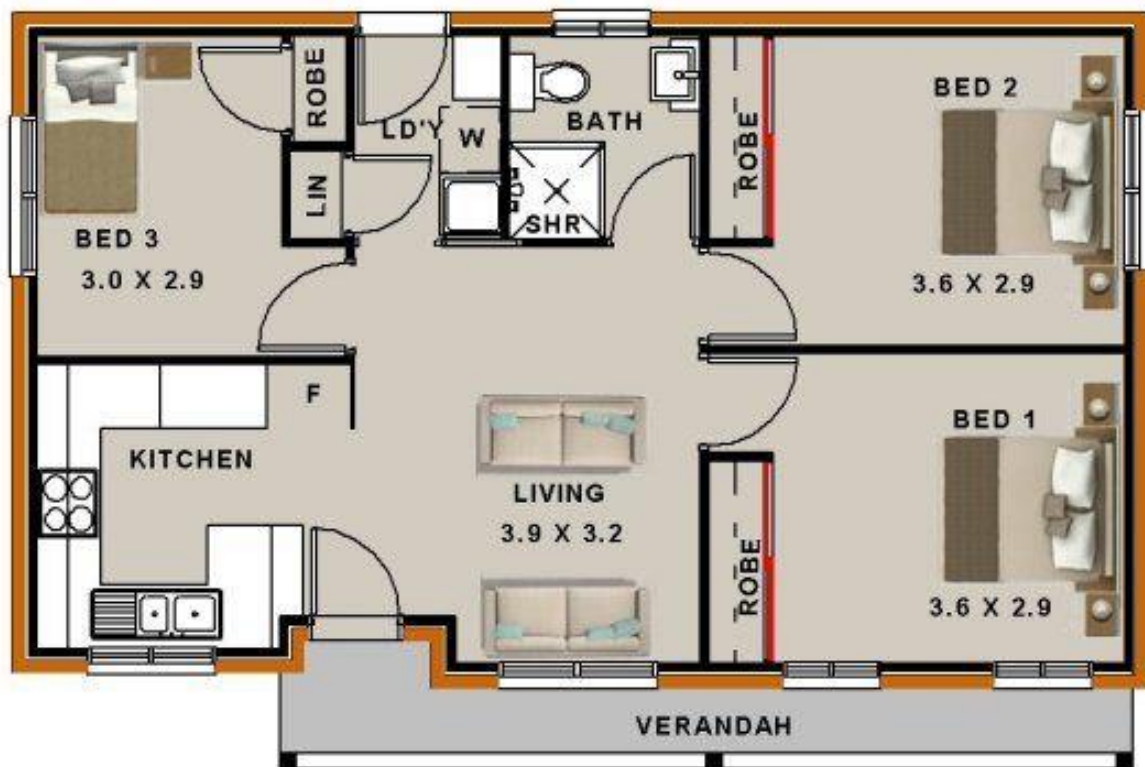
A production order to Facebook for *basic subscriber information* leads to the IP address 86.105.22.100 (Romanian); the IP address is used on 2028-09-11 11:30:47 am UTC to create the FB profile.

The *basic subscriber information* received from FB also shows the mobile number +1 (415) 555-2671 and the Gmail account paradiselost97@gmail.com. A request to Google leads to an identifiable IP address of 81.245.44.54 which is in your capital; This IP address was last used on 2029-04-06 09:23:47 am (UTC) to access the Gmail account. According to the Internet Service Provider, the IP address was assigned to a person named **Alice**, living at Elmstreet 666 of your capital. According to the national registry 2 people are living at the identified physical address: **Bob** and **Alice**. According to confidential information from State Security, **Bob** and **Sam** visited a few months ago the same radicalized mosque where the *salafiya jihadiya*⁴ was being preached. **Bob** was photographed with Abu Jihad.

Finally, on 10 April 2029 a house search is initiated in the ground floor apartment of Elmstreet 666 in your capital.

⁴ Salafia Jihadia is a Salafi jihadist militant group based in Morocco and Spain with links to Al-Qaeda. [Wikipedia.org]

2.2 The house search

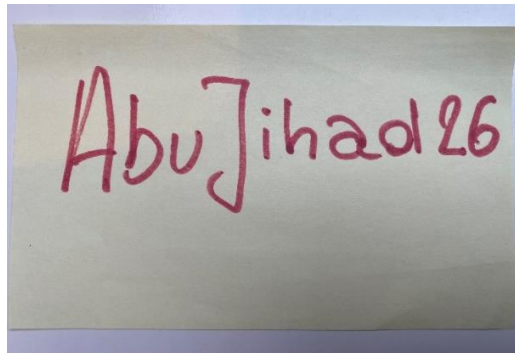


A house search is being carried out. **Sam** and **Bob** are present, both sitting in the living room, and arrested. The shower basin and the toilet in the bathroom have traces of what later will be identified as TATP⁵. Seven AK47 chargers are seized from the closet of bedroom 3, as well as a flag of IS/Daesh in the living room. **Sam** is in the possession of a smartphone (sp1), and **Bob** seemed to be in the possession of two smartphones (one in his pocket (sp2) and one in front of him on the desk he was sitting at when entering the apartment (sp3)). The smartphones are seized and put in a faraday bag.

2.2.1 The living

In the living room, the police discover a laptop (lt1), which is locked. On the keyboard there is a post-it which mentions "AbuJihad26", which could be a password:

⁵ Triacetone triperoxide (TATP) is the trimer of Acetone peroxide (also called APEX) which is an organic peroxide and a primary high explosive.[Wikipedia.org]



The police try the password and the laptop opens. On the screen, the police observe a session with a connected NAS-server (nas1) in which files, pictures and documents are stored. Apparently, this is about a reconnaissance that was carried out in and around the national airport. The police ask **Sam** and **Bob** about the location of the NAS-server. **Sam** says that the NAS-server is in a location abroad, he doesn't want to disclose. Agent Peggy and Victor check the router (rt1), which indicates that the NAS-server should be in the house.

There is also a desktop (pc1) in the living room; **Bob** was behind it when the police entered the apartment Bob initiated a format the storage media, which was successful.. Apparently, there was a discussion between the police and the prosecutor about how to enter the apartment, and they lost valuable time. The police wanted to use force and a flash bang. The prosecutor preferred a soft entry. Anyway, the formatting was successful and the forensic experts are asked to see if something could be recovered.

Further, the police witnessed how **Bob** also tried to switch off the smartphone (sp3) that was lying in front of him on the desk next to formatted desktop computer. The police could seize the smartphone in time, but find that it is locked.

2.2.2 Bedroom 1

In the bedroom of **Alice** there is a desktop (pc2) running, which is unlocked. When they touch the keyboard, the screen opens and they see an opened Yahoo account named [Alice in wonderland 72@yahoo.com](mailto:Alice%20in%20wonderland%2072@yahoo.com), and a Telegram desktop application which shows several group chats.

Sam seems to be willing to cooperate as far as it concerns the Yahoo account; he seems to be afraid and apparently knows that the police can enter the account, since it is open. He states that the account is some sort of shared account by him, **Alice** and **Bob**. He states that he even knows the password of the account. He gives voluntary consent to perform a search in the Yahoo account. He also discloses the password of the Yahoo account for future use, if required.

The police decide to conduct live forensics and they enter the draft folder, sent items folder and inbox of the Yahoo account; in the inbox they find an email with an audio attachment which is encrypted and an email that indicates that a terrorist attack is in preparation. The mails have been sent with the email address abujihad.al.sham@protonmail.com. The police analyse the header information. Based on the imminent threat procedure, Protonmail is requested to release basic subscriber information and available traffic data, but they answer that they don't keep any log files and have nothing to release.

Since the police received the password of the shared Yahoo account, voluntarily from **Sam**, they decide to try to find out if they can login to the connected Flickr account. Due to the fact that the password was voluntarily given by **Sam** for the Yahoo account, and there could be an issue because **Alice** and **Bob** did not voluntarily disclose the used password of the (so called) shared account, the prosecutor decides to apply for a warrant to enter the Flickr account. The judge issues a warrant. They successfully log in to the Flickr account via the police computer. The Flickr account, connected to the Yahoo account, contains a mass of Daesh propaganda material and a draft of a video claiming to be a terrorist attack on the national airport. It seems to be crucial evidence.

With regard to the opened Telegram application, the police map the relevant group names in which terrorist propaganda is disseminated. One conversation in which *@aliceinwonderland_72* is discussing the plans for an upcoming terrorist attack with *@therealabubakr*. A request for expedited preservation of stored computer data and expedited disclosure of preserved traffic data is being sent to Telegram. No answer is given. Telegram does not cooperate, but they do take down the groups listed in the request and they take down the account *@therealabubakr*. The police are left with only screen shots as evidence.

On the same desktop (pc2) the police find a folder called “Kaboom” on the C-drive, in which they find accurate manuals on how to build a TATP bomb, as well as instruction and test videos apparently recorded in the Daesh warzone by Daesh members.

2.2.3 Bedroom 2

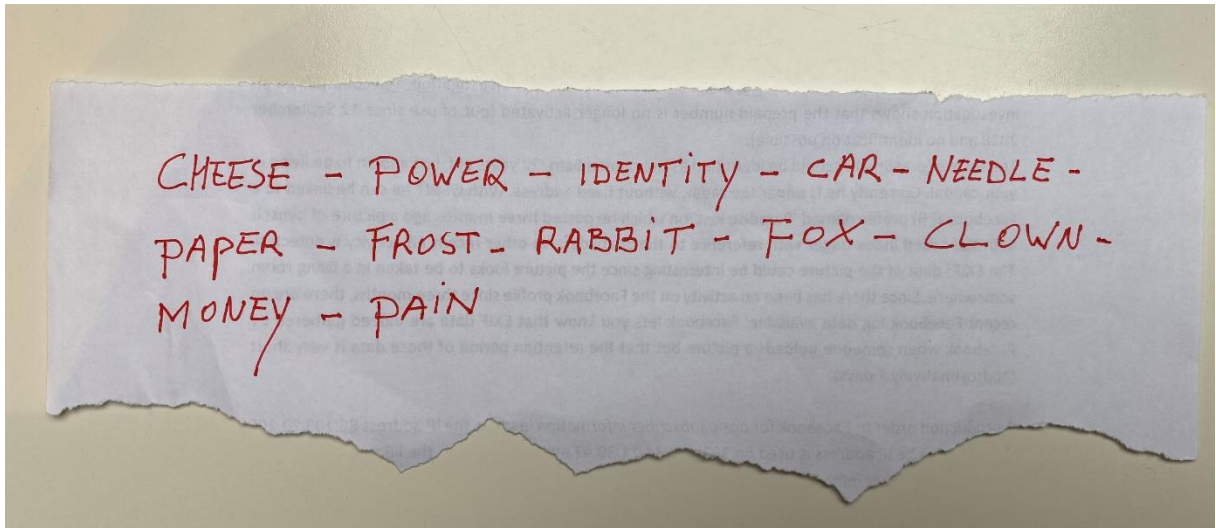
In the bedroom that appears to be **Sam**’s, the tactical team finds a tablet (tb1), which is seized. They notice that strange enough the tablet does not seem to be password protected since it opens as one of the police officers swipe to the left over the screen. The police officer notices that the Whatsapp application is open and that an interesting group chat is going on with an exchange of documents and photos related to preparatory acts for a terrorist attack. The police officer decides to observe the communication for the time being and to save the documents and photos in a folder on the tablet. Further he goes through the photo folder and all other folders to look for relevant information.

After the search, once back in the office, he hands over the tablet to the forensic team, mentioning that he was lucky to save the evidence resolving from the Whatsapp group chat, because meanwhile the exchanged documents and pictures were erased in the group chat.

Based on this information, the prosecutor asks the judge to issue a production order/warrant to WhatsApp to obtain basic subscriber information and log data with regard to the participants of the (empty) group chat. WhatsApp is able to offer an IP address 2001:0db8:85a3:0000:0000:8a2e:0370:7334, which will lead to the identification, localization and arrest of **Alice** on 15 April 2029.

2.2.4 Bedroom 3

In the bedroom of **Bob**, in the drawer of the night table, the police find the following, what looks like a 'seed phrase' of a bitcoin wallet:



Further, also another laptop (lt2) is found and seized in **Bob's** bedroom. The laptop is not turned on. The forensic team dusts the laptop for fingerprints. After forensic analysis of the computer system it seems to contain overwhelming evidence; it contains several folders with, amongst others, farewell letters from martyrs, instructions to build a TATP explosive, and even illegally obtained police records and intercepted police communication...

The investigators question **Bob**, who denies that he knows anything about that laptop. He says that the laptop has been accidentally left by a person called **Eve**, a friend of **Alice**, who just stayed over for two nights, and that she just left yesterday. Bob says that he does not have a clue who Eve might be; he just took the laptop she left to give to Alice on her return. He says he did not use in the laptop, in any way.

Agent Peggy and Victor, of the forensic team of the national police, verify the router logs and discover that the laptop was first connected to the WiFi network of the apartment on **19 March 2029**.

3 Lesson plans

3.1 Lesson: 0 – Course Opening	Duration: 15-60 Minutes
<p>Resources required:</p> <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access (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 • Printer to print the leaflet • Files: Session 0 – Course Opening.pptx, Session 0 - Leaflet.docx 	
<p>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.</p>	
<p>Objectives:</p> <p>By the end of the lesson the students will be able to:</p> <ul style="list-style-type: none"> • Identify the trainers and fellow delegates • Discuss the overall aim of the course • List the modules and activities of the timetable • List the health and safety procedures for the venue 	
<p>Introduction</p> <p>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.</p> <p>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.</p> <p>All information about this session is included in the PowerPoint presentation entitled “Session 0 – Course Opening.pptx” in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.</p> <p>Depending on the number of participants and the intensity of the introduction exercise the length of this session varies between 15 minutes (very brief or no introductions) to 60 minutes (partner interviews and mutual introduction with leaflets). Note that Session 1 foresees some buffer to compensate for a longer introduction.</p>	
<p>Practical Exercises</p> <p>The only practical exercise in this session is the introduction of the delegates and trainers. This should be conducted in a structured manner. It is good practise to allow time for mutual introductions whenever multiple nations or just different entities from the same country participate in the course. Time spent on proper introductions will be rewarded by participants</p>	

who network more, are more engaged and motivated to learn and contribute during the course. This also helps to break the ice at the beginning of the course. A leaflet "[Session 0 - Leaflet.docx](#)" has been produced as an example for an introduction leaflet.

3.2 Lesson: 1 – Introduction to Electronic Evidence

Duration:
60 Minutes

Resources required:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (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
- Printer to print the leaflet
- Files: [Session 1 – Introduction to Electronic Evidence.pptx](#)

Aim: To raise awareness about the importance of electronic evidence to all criminal proceedings and to highlight the availability of international tools providing guidance and help on fighting cybercrime and handling electronic evidence. The participants should also learn all steps involved in the lifecycle of electronic evidence.

Objectives:

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

- Explain the importance of electronic evidence to all criminal proceedings
- Discuss the international landscape around electronic evidence
- Describe the lifecycle of electronic evidence

Introduction

This session is a session on introductory level. It is intended to set the frame for the next sessions and to put the whole training into a context.

Ideally the participants should have passed the "Introductory course on cybercrime and electronic evidence for judges and prosecutors". Thus, they should already have a good understanding about cybercrime, the technology involved and electronic evidence. However, they might not be aware of all the tools and their updates produced by the CoE.

It is important to note that even though Sessions 1 to 3 of this course may focus on theoretical aspects, the course itself will be very practical because one of the core elements of the course will be a case scenario which not only needs to be solved but also needs to be conclude in an evidential hearing (Mock Trial light).

All information about this session is included in the PowerPoint presentation entitled "[Session 1 – Introduction of Electronic Evidence.pptx](#)" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is no practical exercise foreseen in this session. However, to gain more interaction from the class, the trainer could hand out moderation cards, asking the participants to give examples of cases involving electronic evidence. The trainer could also hand out copies of the tools developed by the CoE (Cybercrime Convention, Electronic Evidence Guide, etc) and ask the participants to provide examples and good practise for the steps involved in the lifecycle of electronic evidence.

3.3 Lesson: 2 – Refresher Course on the Convention on Cybercrime (Budapest Convention)	Duration: 210 Minutes ⁶
<p>Resources required for an off-line delivery:</p> <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access (if available) • Whiteboard • Whiteboard pens (at least 2 each of blue, black, red and green) • 2 Flipcharts with adequate paper • Student notepaper and pens • Blu tack or a similar product to allow for paper to be affixed to the walls temporarily • Files: Session 2 Refresher Course BC.pptx <p>Resources required for an on-line delivery:</p> <ul style="list-style-type: none"> • Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability • A strong internet connection • An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms. • Files: Session 2 Refresher Course BC.pptx 	
<p>Aim: The aim of this course is to familiarize all trainees with the Convention on Cybercrime. Those who have recently received the basic and specialised training can get a much shorter overview. In any case, it is important to approach the Convention on Cybercrime as a "toolbox" with regard the collection of electronic evidence and its use in court.</p>	
<p>Objectives:</p> <p>At the end of this session, delegates will be able to:</p> <ul style="list-style-type: none"> • Provide an updated picture of the reach of the Convention on Cybercrime • Know how the Convention on Cybercrime is structured • Find their way into the provisions of the Convention on Cybercrime 	

⁶ this can be reduced to 120 minutes depending on how recently the participants completed the IJT and AJT courses

- Know which articles of the Convention on Cybercrime are specifically important for the collection of electronic evidence

Introduction

The purpose of this presentation is to go through the contents of the Council of Europe Convention on Cybercrime (ETS 185) article by article.

When reviewing the articles, it is important to mention from the beginning that as far as the Specialized Course on Electronic Evidence is concerned, it is not the intention to dwell on every article for a very long time, because this has in fact already been done in the basic and specialized courses (IJT and AJT courses).

However, the intention is to approach the Convention on Cybercrime specifically with regard to the collection of electronic evidence and its use in court.

It will therefore need to be explored:

- Reach and scope of the Convention on Cybercrime
- Definitions
- Three major sections of the Convention on Cybercrime (Substantive law, Procedural law and International Cooperation)

In view of the fact that there is also specialised training on international cooperation, which will specifically focus on the collection of electronic evidence abroad, it should be underlined that the focus will be on the collection and assessment of electronic evidence at the national level.

A focus will therefore be placed on the central part of the Convention on Cybercrime.

All information about this session is included in the PowerPoint presentation entitled "[Session 2 Refresher Course BC.pptx](#)" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is no practical exercise foreseen in this session.

However, to gain more interaction from the class, the trainer can do the following:

- Ask trainees whether they are familiar with the Convention on Cybercrime and whether they have already used it in practice and which articles they have mainly used.
- Give a number of examples from their own experience and identify which concrete articles of the Convention on Cybercrime were the most important in this respect
- Handing out the handy pocket version of the Convention on Cybercrime to the trainees and inviting them to go through it at some point in order to determine the structure of the Budapest Convention for themselves.

3.4 Lesson: 3 – Civil liberties and safeguards with respect to electronic evidence	Duration: 45 Minutes
<p>Resources required for an off-line delivery:</p> <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access • Whiteboard • Whiteboard pens (at least 2 each of blue, black, red and green) • 1 Flipchart with adequate paper • Student notepaper and pens • Blu tack or a similar product to allow for paper to be affixed to the walls temporarily • Files: <ul style="list-style-type: none"> ◦ Session 3 Civil Liberties and Safeguards.pptx ◦ Nemo tenetur – ECHR.docx <p>Resources required for an on-line delivery:</p> <ul style="list-style-type: none"> • Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability • A strong internet connection • An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms. • Files: <ul style="list-style-type: none"> ◦ Session 3 Civil Liberties and Safeguards.pptx ◦ Nemo tenetur – ECHR.docx 	
<p>Aim: Through the previous training sessions, the trainees already had an introduction to electronic evidence (session 1) and a profound refresher on the Budapest Convention principles and substantive and procedural law provisions have a picture of what the tools of the Convention on Cybercrime offer them (Session 2: Refresher Course on the Budapest Convention). This session will address the very important aspect of human rights and safeguards in the application of the Budapest Convention and the handling of electronic evidence. A conscious decision was made to make this session a separate one, because this topic deserves special and separate attention. The purpose of this session is to put forward a well-defined standard on respect for conditions and safeguards and human rights, and to emphasize its importance.</p>	
<p>Objectives:</p> <p>At the end of this session, delegates will be able to:</p> <ul style="list-style-type: none"> • Explain the importance of conditions and safeguards and the way they can be determined • Understand the importance of ensuring that human rights and safeguards are applied when investigating, making case assessments or when adjudicating cases in which electronic evidence is involved 	

Introduction

The trainers have already explained in detail to the trainees, at this moment of the training, what the toolbox of the Convention on Cybercrime is, what the electronic evidence is and where it can be found and what the legal framework is within which all this should be done.

In this session, special attention will be paid to the conditions and safeguards provided by the rule of law and human rights that are at stake when it comes to gathering electronic evidence.

It is important to recognize that different jurisdictions may have varying standards and safeguards. As part of the objectives of this session, reference will mainly be made to standards that have already been laid down in certain international conventions and that result from certain supranational jurisprudence, without making a universal claim as to how certain safeguards should be implemented in each jurisdiction. However, certain standards and best practices will be put forward in the light of the Budapest Convention. The message should be that the given synthesis can be adapted to each country taking into account the particularities of the country's legal system and of its legal international commitments.

In the first part of this session, the relationship of the Budapest Convention to other international legal instruments will be discussed from a human rights point of view. The scope of article 15 of the Budapest Convention and the conditions and safeguards that are envisaged will also be discussed. There will also be a very concrete reference to the human rights and safeguards that are addressed.

The second part of this session will mainly focus on the doctrine of the European Court of Human Rights. This may seem to some jurisdictions as if it does not belong to their domestic legal order, but it does belong to the common good of what the Budapest Convention aims for in terms of human rights and safeguards in a generic way. National differences can certainly be discussed, but it should be made clear that there is a minimum standard.

The third part of this session deals with some of the ECtHR's most important case law on electronic evidence and zooms in on what the ECtHR considers important when collecting electronic evidence. It is a non-exhaustive anthology of jurisprudence and principles that must be observed. It is not intended to come across as imperialistic in this respect, but to give a clear direction.

It is important that the trainers/experts go through the summaries of the jurisprudence and give a clear explanation of the context of the jurisprudence. An attempt was also made to indicate when there were dissenting opinions between the judges, which can also make it clear that discussion is always possible.

All information about this session is included in the PowerPoint presentation entitled "[Session 3 Civil Liberties and Safeguards.pptx](#)" in the resource pack. There is also a scientific analysis (Nemo Tenetur - ECHR.docx) of the case law of the ECHR concerning slides 40 and 41, which should enable the trainer/expert to lead a good discussion between the participants. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is no practical exercise foreseen in this session. Anyway, session 3 gives the opportunity to enter into a comprehensive discussion regarding the case law of the ECtHR. More specifically, slides 40 and 41 provide the opportunity to engage in an extensive discussion on the relationship between the right to remain silent and the principle of non-incrimination with regard

to electronic evidence. To this end, for the benefit of the trainers/experts, a very extensive analysis and discussion of the case law of the ECHR in this respect was added. The contribution in question explicitly takes a certain point of view, which can and may, however, be questioned.

3.5 Lesson: 4 - Devices, Networks and Data

Duration:
210 Minutes

Resources required:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (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
- Printer to print the leaflet
- Devices, practical demonstrations of evidential material mentioned in the slides
- Files: Session 4: Devices, Networks and Data.pptx

Aim: This session shall give practical examples of electronic evidence that can be found on different devices. The participants should get an understanding of the potential evidence stored on the devices as well as the evidential value of such evidence. They should also be taught about network services and how to use them.

Objectives:

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

- Explain where electronic evidence may be found
- Discuss the evidential value of hardware items, network devices and other electronically store data
- Describe different services and technology used on the Internet

Introduction

In other CoE courses the focus of the hardware related sessions is on the identification of devices and on the technical description of services on the Internet. This session focusses on the potential evidence which may be found on the different devices as well as the practical usage of services and technologies.

This session covers the following topics:

- Hardware
- Networks
- Internet
- DNS
- IP addresses
- PKI
- Electronic Records
- Data records
- Documents
- Authorizations
- Signatures

- Logs
- Blockchain
- Cryptocurrency
- Darkweb
- Encryption

All information about this session is included in the PowerPoint presentation entitled "[Session 4: Devices, Networks and Data.pptx](#)" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There are practical exercise foreseen in this session. Since these are very short and straightforward exercises, the instructions for them are either included on the respective slides themselves (e.g. slides 22-28) or in the comment section of those slides (e.g. Slide 55).

3.6 Lesson: 5 – Authorisation to collect electronic evidence

Duration:
45 Minutes

Resources required for an off-line delivery:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (if available)
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily
- Files: [Session 5 Authorisation to collect EE.pptx](#)

Resources required for an on-line delivery:

- Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability
- A strong internet connection
- An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms.
- Files: [Session 5 Authorisation to collect EE.pptx](#)

Aim: Through the previous training sessions, the trainees already have a picture of what the tools of the Convention on Cybercrime offer them (Session 2: Refresher Course on the Budapest Convention), the digital evidence to which these tools are applied (Session 4: Devices, Networks and Data) and the boundaries within which they should work (Session 3: Civil Liberties and Safeguards with respect to Electronic Evidence). This session will now provide a concrete legal explanation of how to obtain electronic evidence by drafting applications for prior authorisation. These applications must meet various criteria, which will be discussed in detail during this session.

Objectives:

At the end of this session, delegates will be able to:

- Recognize particular considerations relating to the **drafting of applications** for exercise of electronic evidence procedural powers and the seeking of **prior authorisation**
- Realize the **contents** of a typical application including scope & duration and other requests
- Understand **what to look for** in an application seeking exercise of electronic evidence procedural powers and seeking authorisation
- Understand some of the **considerations and safeguards** that should be kept in mind when drafting and looking at applications for exercise of electronic evidence procedural powers and seeking authorisation

Introduction

The trainers have already explained in detail to the trainees, at this moment of the training, what the toolbox of the Convention on Cybercrime is, what the electronic evidence is and where it can be found and what the legal framework is within which all this should be done.

In this session it should be made clear that the exercise of the procedural powers should take place within a framework where there is a prior authorisation from the competent authorities (in most countries, a judge).

This means that the petitioner knows and is taught what the content of such a request is and why the content is relevant for, on the one hand, allowing privacy invasive measures and, on the other hand, strictly monitoring the impact of these rights.

In the first part of this session, by way of introduction, we will once again very briefly consider what is available in the Budapest Convention. What measures are interesting for obtaining electronic evidence and where are the safeguards in the Budapest Convention to allow this? It is also clarified that these safeguards are necessary and relevant throughout the process. This part can be gone through quickly, because it is a short repetition.

The second part deals with what should be included in such a petition (clearly stating that this may vary from country to country and jurisdiction to jurisdiction, but that the essence of the content should be the same). A concrete example is also shown.

It is emphasised that a request must be clear, very specific and limited in scope and duration. The second part focuses on the formal aspect.

The third part focuses on the substance of the petition and why the conditions and safeguards are contained in the petition. The focus is on the protection of privacy. Slide 39 certainly requires sufficient attention because, in addition to the protection of privacy, certain data also require special protection because they relate to the journalistic secrecy of the source, the professional secrecy of a doctor or lawyer or the freedom of religion.

All information about this session is included in the PowerPoint presentation entitled "Session 5 Authorisation to collect EE.pptx" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is no practical exercise foreseen in this session. However, to gain more interaction from the class, the trainer could do the following (it should be borne in mind that only 45 minutes are available for this session):

- Slide 13 provides an example of a network search authorisation. This mandate is also part of the training material. This mandate can therefore be handed out and reviewed.
- Trainees may comment on the extent to which they feel that this authorisation is in line with what they expect from such an authorisation, after having followed the training of this session, and with what they are accustomed to in their country from their experience. This exercise may be held at the end of the training of session 5, depending on the time still available.

3.7 Lesson: 6 – Collection of electronic evidence

Duration:
150 Minutes

Resources required for an off-line delivery:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (if available)
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily
- Files: [Session 6 Collection of Electronic Evidence.pptx](#)

Resources required for an on-line delivery:

- Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability
- A strong internet connection
- An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms.
- Files: [Session 6 Collection of EE.pptx](#)

Aim: This session will cover the technical principles of the collection of electronic evidence. Although these principles remain largely similar across jurisdictions, this course has been developed with the aim of standardising our approach and is based on internationally recognised international standards such as ISO/IEC 27037 and the NIST Guide to Integrating Forensic Techniques into Incident Response.

Objectives:

At the end of this session, delegates will be able to:

- Explain which measures need to be taken in order to preserve evidence and prepare for its collection
- Identify sources of electronic evidence
- Discuss options for recovery of data from physical storage media as well as cloud storage
- Be aware of the challenges posed by encryption
- Describe the processes of seizing, imaging and hashing data
- Distinguish between Live data forensics and post mortem forensics
- Illustrate the importance of the chain of custody
- Discuss data retention policies

Introduction

In other CoE courses the focus of the hardware related sessions is on the identification of devices, the technical description of services on the Internet and the potential evidence which may be found on the different devices as well as the practical usage of services and technologies. This session focusses on how to prepare for the capture and how to collect that evidence from different devices and world wide web services.

This session covers the following topics:

- Preservation of evidence
- Preparation for collection
- Identification of evidence
- Recovery from physical storage devices
- Recovery forensics from the cloud
- System administrators
- Encryption and decryption
- Seizure of systems and devices
- Imaging
- Hashing
- Live forensics vs dead (post-mortem) forensics
- Chain of custody of electronic evidence
- Data retention

All information about this session is included in the PowerPoint presentation entitled "[Session 6: Collection of electronic evidence.pptx](#)" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is only one small practical exercise foreseen in this session. Since this is very short and straightforward exercises, the instructions for them are included on slide 6 and in the comment section of slide 7.

3.8 Lesson: 7 – Video	Duration: 20 Minutes
<p>Resources required for an off-line delivery:</p> <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access (if available) • Whiteboard • Whiteboard pens (at least 2 each of blue, black, red and green) • 2 Flipcharts with adequate paper • Student notepaper and pens • Blu tack or a similar product to allow for paper to be affixed to the walls temporarily • Files: Session 7 Video.pptx and Electronic Evidence Course V4.mov <p>Resources required for an on-line delivery:</p> <ul style="list-style-type: none"> • Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability • A strong internet connection • An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms. <p>This online tool should also have the ability to share a video live.</p> <ul style="list-style-type: none"> • Files: Session 7 Video.pptx and Electronic Evidence Course V4.mov 	
<p>Aim: The intention is to show the trainees a video of a police raid in a terrorism case (the one of session 9 that they will later get, written down on paper / in a digital file). It is a film made with the help of real police officers and real forensic experts. The suspects are actors. Although it is an acted representation of a case, it could be a real case in the sense that it is a realistic representation.</p>	
<p>Objectives:</p> <p>At the end of this session, delegates will:</p> <ul style="list-style-type: none"> • have a view on how things work in practice • have a picture of what a crime scene looks like and to what extent that crime scene is also a digital crime scene • be able to use this visual representation to get started with the practical exercise 	
<p>Introduction</p> <p>Session 7 consists essentially of showing a video in which the trainees will be confronted with a real case, which was reenacted by actors (role of the suspects) with the help of real police officers and real forensic experts.</p> <p>This case will also be discussed in detail later on, and the trainees will receive the entire scenario in session 9 for further processing.</p> <p>The case concerns a raid in the context of a terrorism case.</p> <p>No terrorist attack has yet been committed, but the police will establish through the seizure and forensic analysis of smartphones, tablets and computers that their intervention was just in time.</p>	

Of course, it is important that the trainees' attention is specifically drawn to the digital evidence and how it is collected.

This is the reason (see also practical exercise) that trainees are asked to take note for themselves (this also increases their attention).

Practical Exercises

There is a practical exercise in the sense that trainees are asked to watch the video very carefully and to take note for themselves of what they notice.

Do they recognize the digital evidence?

Do they already have a view on how the digital evidence is handled?

Is this good or bad according to them?

What about the coercion exerted on the suspects.

The practical exercise will be started in session 7 to be dealt with further in session 8.

It may be a good idea to show the film in its entirety for the first time and if time permits, to play it again afterwards in view of what will happen in session 8 and to pause at some scenes.

3.9 Lesson: 8 – Practical Exercise (Phase 1 – Collection of Electronic Evidence)

**Duration:
30 Minutes**

Resources required for an off-line delivery:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (if available)
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily
- Files: [Session 8 Practical Exercise.pptx](#)

Resources required for an on-line delivery:

- Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability
- A strong internet connection
- An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms.
- Files: [Session 8 Practical Exercise.pptx](#)

Aim: The intention now is to work very concretely with what the trainees saw during the projection of the film in session 7 and what they also kept notes of for themselves. The discussion will be led by showing freeze frames related to the digital evidence and using questions suggested in the next slide.

Objectives:

At the end of this session, delegates will be able to:

- recognize the digital crime scene from a practical and concrete case
- recognize the digital evidence material present
- be able to make a first reflection on how to deal with this.
- be able to make an early critical reflection on possible errors in the handling of this evidence
- question what legitimate measures may be taken to force a suspect to disclose access to digital evidence material

Introduction

In session 8, the trainees will be guided and coached by the trainer to work with what they saw in the film in session 7.

At best, in session 7 the attention is already drawn to the parts of the film that are relevant for the assessment of the digital evidence. In any case, based on freeze frames and suggested questions, they will now discuss and comment on the digital crime scene and how it has been handled.

Please note. The way in which digital evidence was handled in the film is far from ideal. It may answer to the practice in some countries, but it is not an example of how it should be done perfectly. The film is therefore not an example of how to handle digital evidence perfectly, but it is a source for discussion and critical questioning on every action that has been seen.

This is therefore the task of the trainer who also receives further instructions in the slides accompanying the comments.

All further information about this session is included in the PowerPoint presentation entitled "[Session 8 Practical Exercise.pptx](#)" in the resource pack.

The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

This is a practical exercise as the trainees assisted by the trainer get to work with some excerpts from the video of session 7.

Concretely a freeze frame is shown from the movie and the next slide is the slide with the questions that can be asked regarding this image.

It is an important moment for interaction and the trainer's task is to encourage discussion and sometimes play "devil's advocate" where necessary.

3.10 Lesson: 9 – Practical Exercise (Phase 2 – Assessment of Electronic Evidence)	Duration: 120 Minutes
Resources required: <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access (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 • Printer to print the leaflet • Files: <u>Session 9 – Phase 2 – Assessment of Electronic Evidence.pptx</u> 	
Aim:	
Objectives: By the end of the lesson the students will be able to: <ul style="list-style-type: none"> • 	
Introduction This session is a practical session on the assessment of electronic evidence. The participants will all receive a realistic case file (paperless) that contains basically all electronic evidence that has been gathered in this specific case scenario Some organisational information about this session is included in the PowerPoint presentation entitled " <u>Session 9 – Phase 2 – Assessment of Electronic Evidence.pptx</u> " in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.	
Practical Exercises Each group will include four people who will argue that certain evidence should be used in court, and four who will oppose the use of evidence in court [50-50]. The participants will, in addition to other materials already provided (i.e. authorisation, information on how evidence was collected), depending on what stage of the course this exercise will be conducted, also be provided with copy of analysis and possibly even forensic reports. Each group will have a debate /discussion on whether the evidence should be presented, based on the scope of the authorisation and the manner it was collected. This proposed structure for a practical exercise will be neutral in terms of legal systems and would be relevant in all target countries. The experts can overview and moderate the discussions, asking relevant questions if and when required. The participants will all receive a realistic case file (paperless) that contains basically all electronic evidence that has been gathered in this specific case scenario: <ul style="list-style-type: none"> - log files - results of production orders - electronic evidence gathered with a remote (transborder) search and seizure - electronic evidence found on a smartphone that was unlocked by using face recognition (against the suspects will?) 	

- statements of the defendant(s) saying that the evidence has been planted by the police
- hashed electronic evidence
- electronic evidence that has not been hashed
- electronic evidence gathered through live-forensics on a running laptop
- electronic evidence from a cloud-server without know location
- the seizure of a bitcoin seed
- IT-expert reports -...

Thus, in this phase the participants – although divided in groups (one half defends the evidence, the other half attacks it ('The Devil's Advocate')) – will observe/investigate on the same material and will have to accomplish the same investigative tasks and will have to deal with the same electronic evidence challenges and problems.

Group 1	Group 1.A: attack	Group 1.B: defend
Group 2	Group 2.A: attack	Group 2.B: defend
Group 3	Group 3.A: attack	Group 3.B: defend

The discussions within the groups are moderated and guided by an expert. There will be one IT- expert/specialized LE officer, who can be called in by any group to clarify technical questions or issues where needed.

3.11 Lesson: 10 – Examination and analysis of electronic evidence

Duration:
120 Minutes

Resources required for an off-line delivery:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (if available)
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily
- Files: [Session 10 - Examination and Analysis of Electronic Evidence.pptx](#)
[forensic analysis examination 1 voice over.mp4](#)
[forensic analysis examination 2 voice over.mp4](#)
[forensic analysis ram sneakpeak voice over.mp4](#)
[forensic analysis registry voice over.mp4](#)

Resources required for an on-line delivery:

- Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability
- A strong internet connection
- An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms.

- Files: [Session 10 - Examination and Analysis of Electronic Evidence.pptx](#)

Aim: This session will showcase examples of techniques that can be used to examine analyse computer and mobile systems. The participants should get a better overview of what is possible in digital forensics and which evidential data can be extracted from computer and mobile systems.

Objectives:

At the end of this session, delegates will be able to:

- Distinguish between traditional computer forensics and mobile forensics
- Discuss options for the storage of digital evidence
- Describe considerations for determining the volatility
- Outline procedures to collect log files
- Summarise the evidential items which can be found digital devices
- Summarise options for decrypting data
- Discuss different documentation techniques
- Identify methods for physical and logical extractions
- Distinguish between different levels of examinations and analysis techniques
- Describe techniques to analyse hidden data, application data and files
- Identify methods to analyse e-mail evidence and network traces
- Summarise the elements of a forensic report

Introduction

This session is split in three parts. The first short introductory part shows the different areas in the field of digital forensics and outlines some of the differences between computer forensics and mobile forensics. The second part will give examples of challenges, analysis techniques and evidential items that can be found when analysing a computer system. The third part has a similar focus as the second part, but it concentrates on mobile devices.

This session covers the following topics:

- Storage of evidence
- Determination of volatility
- Collection logs
- Decryption
- Documentation
- Physical & logical extraction
- Temporal analysis
- Relational analysis
- Functional analysis
- Timeframe analysis
- Data hiding analysis
- Application and file analysis
- Log Files analysis
- Email analysis
- Network analysis
- Preparation of report (scope, contents, organisation)

All information about this session is included in the PowerPoint presentation entitled "[Session 10 - Examination and Analysis of Electronic Evidence.pptx](#)" in the resource pack. There are also pre-recorded videos available for this session:

[forensic analysis examination 1 voice over.mp4](#)

[forensic analysis examination 2 voice over.mp4](#)

[forensic analysis ram sneakpeak voice over.mp4](#)

forensic analysis registry voice over.mp4

The trainer can use them throughout part 2. There are notes in some slides indicating a potential use of a video.

The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is no practical exercise in this session. However, an experienced trainer can decide to deliver the whole session via live demo showcasing the analysis of a case in a forensic software.

3.12 Lesson: 11 – Preparation of Electronic Evidence for Court

Duration:
45 Minutes

Resources required for an off-line delivery:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 1 Flipchart with adequate paper
- Student notepaper and pens
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily
- Files:
 - [Session 11 Preparation of Electronic Evidence for Court.pptx](#)

Resources required for an on-line delivery:

- Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability
- A strong internet connection
- An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms.
- Files:
 - [Session 11 Preparation of Electronic Evidence for Court.pptx](#)

Aim:

The purpose of this session is to bring to the attention of the participants what they need to think about when preparing their case for court. It is important that it is made clear to them that this is **an evidentiary hearing**, and that guilt or innocence is therefore not addressed. It only concerns the admissibility and integrity of the electronic evidence. Considerations will be given to the participants to enable them to prepare their case (attack/defend) in a well-considered, punctual and creative way for the hearing.

Objectives:

At the end of this session, delegates will be able to:

- Manage and plan prosecution and defence

- Deal with arguments on admissibility of electronic and other evidence
- Choose methods for presenting electronic evidence in court

Introduction

First of all, it will be made clear to the participants that they need to prepare for an evidentiary hearing, and that the debate is therefore limited to the admissibility of the electronic evidence. Discussions about guilt or innocence are not allowed. Only the (electronic) evidence, its admissibility, its integrity, its credibility are at stake.

Furthermore, some general observations are made with regard to going to court, such as to consider combining adversarial and inquisitorial approaches, and how to manage prosecution and defence. It will be brought under the attention of the participants that classically, the defence has it a little easier: the defence can often afford to launch an attack against any facet of evidence. The defence has to sow doubt and can and may go very far in doing so. In other words, the defence sometimes has the luxury of being destructive. The public prosecutor, on the other hand, always has the task of constructively building up the evidence.

Further, the assessment criteria of the reliability and authenticity of electronic evidence is brought under the attention of the participants, as well that they should be ready to deal with jurisdictional issues, especially with regard to electronic evidence that was gathered cross border. The defence team should think about how to develop defence arguments on that subject. The prosecution team should think about how to defend cross border electronic evidence.

Finally, we will elaborate on the way in which the arguments concerning the electronic evidence can be brought before the court, and which points of interest deserve special attention. Presentation techniques and tools will be brought to the attention. But also the attention for the principles of a fair trial will be emphasized.

This session is meant as a reflection exercise. It is advisable to interact with the participants and ask them "how they would do it" and what they are thinking about.

Practical Exercises

There is no practical exercise foreseen in this session, besides interactive discussion.

3.13 Lesson: 12 – Admissibility of Electronic Evidence

Duration:
120 Minutes

Resources required for an off-line delivery:

- Laptop or PC running an operating system with an office suite (capable of showing pptx)
- Projector and display screen
- Internet access (if available)
- Whiteboard
- Whiteboard pens (at least 2 each of blue, black, red and green)
- 2 Flipcharts with adequate paper
- Student notepaper and pens
- Blu tack or a similar product to allow for paper to be affixed to the walls temporarily
- Files: [Session 12 Admissibility of EE.pptx](#)

Resources required for an on-line delivery:

- Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability
- A strong internet connection
- An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms.
- Files: [Session 12 Admissibility of EE.pptx](#)

Aim: Trainees should be aware that going to court with electronic evidence can only succeed if all parts of the chain in het electronic evidence flowchart have been completed correctly. The assessment and evaluation of the admissibility of electronic evidence is a very important element in this respect before that electronic evidence can be judged. It is, as it were, the penultimate link in the chain. it is a crucial link in the chain.

However well the electronic evidence may be identified, however securely secured, however sound and well-reasoned the prior authorisations may be, however professional the extraction and analysis of the electronic evidence may be, if it is technically and legally inadmissible this electronic evidence, it cannot be used by a judge to make his judgment.

The objective can be achieved by understanding and safeguarding five fundamental principles: the authenticity, completeness, reliability, believability and proportionality of the electronic evidence.

Objectives:

At the end of this session, delegates will be able to:

- distinguish between the technical and legal collection of electronic evidence and the assessment of that same electronic evidence
- understand that as magistrates (public prosecutor or judge) they have a particular important role to play in the assessment of that evidence
- know the different elements with which electronic evidence has to be assessed in order to be admissible before a court and the judgment of a case
- understand that a judge's evaluation of the admissibility of electronic evidence is the cornerstone of the whole process

Introduction

Session 12 deals with the admissibility of the evidence before the court and is therefore the penultimate stage before the digital evidence can be used as evidence by a judge to make his judgment.

The trainees have learned in the previous sessions how to technically access the evidence and within which legal framework and with which tools. The trainees now need to learn how to assess that evidence (in terms of admissibility). They must learn that no matter how good evidence may appear to be, when it is not admissible it is of no value. So, as magistrates, they have a crucial role to play in safeguarding this.

There are three main parts.

In the first stage, it is important to know that the evaluation of the evidence can be different in each country and there are roughly two major systems, the civil law system and the common law system, but there are also hybrid systems.

Secondly, in order to proceed with the requirements of admissibility, it is important to recognize five fundamental principles leading to the admissibility of electronic evidence: authenticity, completeness, reliability, believability and proportionality. These five fundamental principles are explained in more detail in the slides.

As far as the authenticity of the evidence is concerned, an exercise is also linked to this (see below).

Finally, because even fundamental principles have to find their way into practice, the slides put forward five measures to be taken in order to translate these five principles into practice:

1. Safeguarding the **integrity of the data**
2. Creating an **audit trail**
3. Foreseeing **specialist support**
4. Providing **appropriate training**
5. Ensuring **legality**

The content of these slides speaks for itself. In the blue boxes, each time the summary advice is given, it is useful for the trainer to underline this.

All information about this session is included in the PowerPoint presentation entitled "Session 12 Admissibility of EE.pptx" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.

Practical Exercises

There is a practical exercise in the slides 9-12.

As regards the 'authenticity' of electronic evidence, at the level of knowledge of magistrates, it is explained how the calculation of a hash value is a tool that can prove that two files are completely identical and the file submitted to the court is indeed the file that was seized and is therefore authentic.

Slide 9 indeed shows twice the same picture of which the trainer or trainees can calculate the hash value (file "alexander seger.png"). This calculation is possible with freely available tools such as these at <https://www.fileformat.info/tool/hash.htm>. Please pay attention to the SHA-1 as well as the MD5 values.

In slide 10 it is immediately noticeable that the text under the image was changed from "HEAD OF CYBERCRIME DIVISION, COUNCIL OF EUROPE" to "HEAD OF ORGANIZED CRIMEGROUP ARRESTED". It is clear to the trainees that something has changed in the image, but it also becomes clear when calculating the hash value, which is different for both SHA-1 and MD5 ("alexander seger2.png" file).

In slide 11 for the "*die hards*" in the classroom, an example is given of two photos that are undeniably different, but of which the MD5 value turns out to be the same (photos in the teaching package "plane.jpg" and "ship.jpg"). The lesson given here is that the SHA-1 is indeed different and therefore it is best to use more than one calculation method.

This is finally ultimately demonstrated by an example from practice in slide 12. It concerns three photographs from an observation file where two targets were observed and where the hash value SHA-1, MD5 was calculated at the time the specialised police services took the

photograph. The hash values must be the same to prove that Photoshop was not used to put two people together on a photo that they never met in real life.

If there is time left, trainees can be asked whether they are familiar with case law of the European Court of Human Rights on the admissibility of evidence.

There are certainly two interesting and useful references here:

1. CASE OF RAMANAUSKAS v. LITHUANIA, 5 February 2008 (<http://hudoc.echr.coe.int/eng?i=001-84935>)

52. ... The admissibility of evidence is primarily a matter for regulation by national law and, as a rule, it is for the national courts to assess the evidence before them. The Court, for its part, must ascertain whether the proceedings as a whole, including the way in which evidence was taken, were fair (see, among other authorities, Van Mechelen and Others v. the Netherlands, 23 April 1997, § 50, Reports of Judgments and Decisions 1997-III; Teixeira de Castro, cited above, § 34; Sequeira v. Portugal (dec.), no. 73557/01, ECHR 2003-VI; and Shannon v. the United Kingdom (dec.), no. 67537/01, ECHR 2004-IV). In this context, the Court's task is not to determine whether certain items of evidence were obtained unlawfully, but rather to examine whether such "unlawfulness" resulted in the infringement of another right protected by the Convention.

2. CASE OF GÄFGEN v. GERMANY, 1 June 2010 (<http://hudoc.echr.coe.int/eng?i=001-99015>)

164. In determining whether the proceedings as a whole were fair, regard must also be had as to whether the rights of the defence have been respected. In particular, it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use. In addition, the quality of the evidence must be taken into consideration, as must the circumstances in which it was obtained and whether these circumstances cast doubts on its reliability or accuracy. While no problem of fairness necessarily arises where the evidence obtained was unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker (see, inter alia, Khan, cited above, §§ 35 and 37; Allan, cited above, § 43; and the judgment in Jalloh, cited above, § 96). In this connection, the Court further attaches weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (compare, in particular, Khan, cited above, §§ 35 and 37).

3.14 Lesson: 13 – Preparation for Evidentiary Hearing	Duration: 120 Minutes
<p>Resources required:</p> <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access (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 • Printer to print the leaflet • Files: <u>Session 13 – Preparation for Evidentiary Hearing.pptx</u> 	
<p>Aim:</p>	
<p>Objectives: By the end of the lesson the students will be able to:</p> <ul style="list-style-type: none"> • 	
<p>Introduction</p> <p>This session is a practical session on the preparation for an evidential hearing.</p> <p>The participants will continue their work on the case scenario and will prepare their plan, arguments and presentations (for which they can freely choose all means available: outlines, power point presentation, etc.) for the evidentiary hearing that will follow later on.</p> <p>The evidentiary hearings will consist of the prosecution presenting their case and the electronic evidence, while the defence will cross-examine or question the prosecution's (expert)witnesses. Additionally, all motions will be heard by the Court, which typically includes motions to exclude or admit to evidence. The parties will argue over what evidence should or should not be included at trial, as well as whether specific (expert)witnesses should be used at the trial. Further, the defence may also file a motion to dismiss the entirety of the prosecution's case against the defendant. Motions of parties will be shared in real time, also with the judges, so the court and the parties can prepare the hearing.</p> <p>The judges/ judges' team will start to anticipate on potential defence arguments, electronic evidence assessment, the trial preparation, the hearing of witnesses. The judges will establish some basic rules</p> <p>In this phase the experts will point out what will be expected from the participants in the evidentiary hearing. Some information about this session is included in the PowerPoint presentation entitled "<u>Session 13 – Introduction of Electronic Evidence.pptx</u>" in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved.</p>	
<p>Practical Exercises</p> <p>The participants may be divided in one of two different ways, taking into account cultural sensitivities and other factors:</p>	

Option 1:

The participants will be divided in **3 groups**. After phase 2, three groups will be assigned as:

- The prosecution team
- The judges team
- The defence team

Hereby, cultural sensitivities will be taken into account. The groups can be created randomly or on a voluntary basis. If the number of the participants exceeds 30, a plural of three groups could be created, or a second defence or prosecution team could be created. However, it has to be noted that it will make the implementation of the Pre-Trial Hearing more complex. Every group needs to be guided and supported by an expert. Therefore, you will need as many experts as you will create groups (+ 1 additional).

Before the start of this phase, the participants will be shuffled and divided in new groups:

Prosecutors	Group 1.A	Group 2.A
Defence lawyers	Group 1.B	Group 3.B
Judges	Group 3.A	Group 2.B

The shuffling of the groups creates a situation wherein the participants who had to be 'the Devil's Advocate' in the assessment phase, now will have to defend the evidence. Those who defended the evidence in phase 2, now will have to attack it. **Letting the participants rotate**, will challenge the mindset of the participants towards the electronic evidence they assessed in the previous phase.

Depending on the number of participants, the choice can be made to split up the teams, in which case you will have two separate evidentiary hearings in separate rooms:

	Room 1	Room 2
Prosecutors	Group 1.A	Group 2.A
Defence lawyers	Group 1.B	Group 3.B
Judges	Group 3.A	Group 2.B

Option 2:

Participants will be divided into two rooms, each with one expert trainer. Assuming there are 32 participants, each room will have 16 participants. These will be subdivided into four groups of four participants each (a judge, prosecutor, forensic expert/police officer/expert witness, and possibly depending on the legal system a defense counsel). The possibility of two judges in a group may also be explored.

Room 1	Room 2
4 groups, each consisting of:	4 groups, each consisting of:
<ul style="list-style-type: none"> • 1 judge • 1 prosecutor • 1 forensic expert / police officer / expert witness • 1 defence counsel 	<ul style="list-style-type: none"> • 1 judge • 1 prosecutor • 1 forensic expert / police officer / expert witness • 1 defence counsel

It is recommended that both options be included in the course, and depending on cultural sensitivities, the most appropriate group formulation be considered on a country-by-country basis.

As laid out in the "Introduction" of this sessions, the participants will continue their work on the case scenario and will prepare their plan, arguments and presentations for the evidentiary hearing that will follow later on.

3.15 Session 14: Practical Exercise (Phase 3 - Evidentiary Hearing + Phase 4 - Judgement)	Duration: 120 Minutes
Resources required: <ul style="list-style-type: none"> • Laptop or PC running an operating system with an office suite (capable of showing pptx) • Projector and display screen • Internet access (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 • Printer to print the leaflet 	
Aim:	
Objectives: By the end of the lesson the students will be able to: <ul style="list-style-type: none"> • 	
Introduction This session consists of two parts, the evidentiary hearing and the judgement. Both parts are practical sessions. The evidentiary hearing is the grand finale which the participants have been preparing for. Recommendations regarding the organisation of the hearing are provided in the section below.	
Practical Exercises The groups as set up in Session 13 will bring their case to court. Phase 1: Hearing The format of the evidentiary hearing will depend on the group formation selected, though in principle, the hearings will be similar irrespective of group formation. If the participants are divided into prosecution, defence lawyer and judges teams, during the evidentiary hearing, two or three team leaders (depending on the results within the group, etc.) of the prosecution team will present their case and the electronic evidence. The team can also divide tasks, motions and statements at its own discretion. The defence team will have the	

possibility to file motions and present their arguments. Within the judges' team, a president of the court has to be assigned who will be responsible for the order in court and the leading of the debates (the expert who guided/supported the judges team, can be a 'judge assessor'). Throughout the evidentiary hearing phase, the judges team will steer very carefully and set out the debate and discussions in court to the point that every participant will end up with the right lessons learned. The expert witness (an IT expert/LE officer) can be questioned (cross examination is possible) in court by the judges, the defence team and the prosecution team.

If the participants are divided into teams each consisting of a judge, prosecutor, witness and defence counsel, each team member will have an opportunity to play each role.

Action and reaction is key in this phase.

In the development of the material, common law and civil law differences can and should be taken into account, but as said, a hybrid approach could be profitable for all participants.

For example: in a civil law system, the cross-examination of expert witnesses, or showing in court where the evidence was found in the device, is not really a common practise. However, any prosecutor or judge from a civil law country would be eager to benefit from the knowledge and expertise resulting from this exercise. Also, in civil law countries, more and more frequently, when requested to execute mutual legal assistance request, prosecutors and judges are requested to follow certain common law requirements in the gathering of the evidence to make sure that the evidence would also be admissible in a common law court.

The goal is that a natural realistic court situation will be created and that discussions and remarks will evolve as in real court situations. The experts are responsible to stimulate the participants to a fluent court discussion, action and reaction.

Phase 2: Judgement/Ruling

After all parties have been heard, the debates are closed and the case is taken into consideration by the court. The judge will not make any ruling on culpability but solely on the evidence after proper examination of the evidence.

Since the judges/judges' team had the opportunity to anticipate on the arguments and make preparations throughout the trial preparation phase, they will be given +/- 45 minutes to come to a judgement.

If the participants are divided into prosecution, defence lawyer and judges teams, during the evidentiary hearing, during this deliberation, the prosecution team and the defence team will debrief the court proceedings for their respective teams and list up their observations.

The judge will come to a final judgement which they will present in plenary. This is basically also a sort of debriefing that is designed to put the evidentiary hearing experience into perspective. The judgement gives a summary of the motions and issues raised and a review of the arguments and legal issues which were brought in the pre-trial procedure. The possibility is left open for individual judges to explain any dissenting opinions that were not withheld by the majority of the judges. Given the time limitation, the judgement or ruling does not have to be formalistic, and could be in the form of a presentation or even bullet points covering the key issues related to electronic evidence.