****

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Data Protection and Cybercrime Division Directorate General of Human Rights and Rule of Law Strasbourg, France  Draft Version 23rd April 2015 |

**Activity 5.2**

**Advanced Cybercrime and Electronic Evidence Training Course for Judges and Prosecutors**

**Training Manual and Resource Pack**



|  |  |
| --- | --- |
| **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](mailto: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 |

**Contents**

Introduction 5

1 General Overview 7

1.1 Aim of the Course 7

1.2 Why is this training necessary 7

1.3 The curriculum 8

2 How to use the trainers guide 8

3 Course Overview 9

3.1 How long is the course and who is it for 9

3.2 Who will deliver the course 9

3.3 How will the course be delivered 10

3.4 Course objectives 10

3.5 Target students and trainers group 10

3.5.1 Students 10

3.5.2 Experience Prerequisites 10

3.5.3 Trainers 10

3.5.4 Experience Prerequisites 10

3.6 Resources 11

3.6.1 Course Resources requirements 11

3.6.2 Course Resources customisation 16

3.7 Assessment 19

3.8 Timetable 20

3.9 Course and lesson objectives 21

4 Key Contacts 24

5 Lesson Plans 25

Lesson: 1.1.1 – Course Opening and Introductions 25

Lesson: 1.1.2 – Developing an Investigation Plan 25

Lesson: 1.1.3 – Introduction to the Case Scenario 26

Lesson: 1.1.4 – Group Work – Identifying Crimes 29

Lesson: 1.1.5 – Feedback on Group Work 30

Lesson: 1.2.1 – Daily Review 31

Lesson: 1.2.2 – Traditional and Alternative Currencies 31

Lesson: 1.2.3 – Group Work – Financial Aspects 32

Lesson: 1.2.4 – Presentation - International Cooperation 33

Lesson: 1.2.5 – Group Work – International Cooperation 34

Lesson: 1.2.6 – Group Work – Identifying the Suspects 35

Lesson: 1.2.7 – Feedback on Group Work 36

Lesson: 1.3.1 – Daily Review 37

Lesson: 1.3.2 – Presentation – Digital Forensics 37

Lesson: 1.2.3 – Group Work – Digital Forensics 38

Lesson: 1.2.4 – Presentation – Preparing the Case for Court 39

Lesson: 1.3.4 – Group Work – Finalising the Case 40

Lesson: 1.2.5 – Case Review – Feedback 41

Lesson: 1.3.6 – Course Closure 41

6 Evaluation 42

7 Assessment 42

# Introduction

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

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

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

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

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

Through the Joint Regional Project of the European Union and Council of Europe CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime)[[1]](#footnote-1), the training institutions from the projects areas (Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, “The former Yugoslav Republic of Macedonia”, Turkey and Kosovo[[2]](#footnote-2)) are supported to implement the training concept.

In this context, training materials have been developed to be used by training institutions, a “Training of Trainers Programme” has been carried out and a regional centre created based in Croatia.

The current (2015) update of the course has been undertaken to ensure that the materials are relevant to other areas of the world. It is intended that the updated training materials will enable the scenario, at the core of the course, to be adapted for delivery in any part of the world. In addition, the presentations have been reviewed to ensure they reflect the learning objectives of each session, as well as updated to take account of changes in technology.

The training materials are now colour coded in order that future trainers are able to see which elements on the course should be amended for delivery in different regions. A separate set of guidelines is included to assist this process. Future updates to the course may enable fully automated changes to the course. An automated update function would be of great advantage and it is anticipated that one may be available by the end of 2015, beginning of 2016. This will allow the scenario dates and other information to be updated more readily.

Under the GLACY project, a further guideline document has been created, entitled “Guidelines for the delivery of Council of Europe judicial training courses on cybercrime and electronic evidence”. The document is available from the Council of Europe website at [www.coe.int/cybercrime](http://www.coe.int/cybercrime). The concept of the COE is to empower countries to develop their own programme by providing the first levels of training and then supporting countries as they incorporate the available training into their programmes. The paper provides information about the available training in order that it may be delivered during and following the involvement of the COE in each country. The report does not repeat the content of the existing material and provides references to that material in order that readers may consider them in conjunction with the information provide therein. The document may be useful for countries that are planning to deliver cybercrime training nationally.

This update of the course is implementing some changes to the training manual. The main change is the incorporation of additional information in the text section of PowerPoint slides, where relevant, and the removal of this information from the lesson plans. The reason for this is very practical. The original course materials were prepared in 2012 and the course has been delivered on several occasions in both English and French languages. It was originally intended that the training pack would be updated after each delivery, however, for a number of reasons this has not taken place. The result is that new and updated relevant information has been delivered during training courses, whereas the training pack has not been updated. This means that training pack is not synchronized with the latest teaching materials. The new procedure should mean that the training pack would still drive the training but not rely on it being updated so regularly. Minor modifications may take place during training preparation and delivery and it is recommended that a major review is undertaken annually when any necessary changes may be incorporated in the training manual.

1. General Overview

## Aim of the Course

This course is designed to build upon the introductory training course for judges and prosecutors developed by the Council of Europe Cyber@IPA project. It will provide judges and prosecutors with additional level of knowledge on cybercrime and electronic evidence. The course will provide legal as well as practical information about the subject matters and concentrate on how these issues impact on the day-to-day work of judges and prosecutors.

* The aim of the course is to provide the knowledge and skills to allow judges and prosecutors to fulfill their roles relating to cybercrime investigations.
* This course is designed to build upon the learning outcomes of the basic cybercrime training course for judges and prosecutors and should be attended only by those that have successfully completed that course.

The course will cover the following subjects:

* Conducting an investigation,
* Identifying the types of crime committed,
* Establishing the location of evidence, witnesses and suspects,
* Traditional and alternative currencies
* Securing evidence in an acceptable way, irrespective of where it is held,
* Preparing for search and seizure activities involving electronic evidence,
* Dealing with digital devices that are part of the investigation,
* Briefing of forensic specialists and others needed to support the investigation phase,
* Preparing for interviews with suspects,
* Presenting cybercrime evidence
* Considering the relevant aspects during the judicial process and trial

## Why is this training necessary

Judges and prosecutors play an important role in the investigation and adjudication of individuals or groups that have committed crimes. With the increased number of incidence where these crimes have a digital element, a need is created for judges and prosecutors to be properly trained to understand the nature of these crimes and to also be aware of the legislation and the instruments for international cooperation available to handle cases of cybercrimes.

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

Cases of cybercrime often require a swift and very efficient international or regional cooperation, which would provide for a timely investigation and prosecution of the perpetrators. As result the training institutions should make the effort to include in their curriculum modules that contain instructions about the instruments of international cooperation that can be used when investigating cybercrime cases including the use of the 24/7 contacts, MLA, Judicial Cooperation Activity, Judicial Cooperation Platforms etc.

## The curriculum

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

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

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

This Training Module is built in such a way that will enable judges and prosecutors that have passed through introductory module to enhance their knowledge of the nature of cybercrime, the terms and the technology by dealing with a practical case scenario from the initial complaint, through the investigation and to the trial process.

This module has been created with the goal of providing the judges and prosecutors with the additional knowledge that can be applied in practice on the functioning of computers and networks, what is cybercrime, cybercrime legislation, jurisdiction, investigative means and electronic evidence, and international cooperation.

This course has been designed as a mixture of taught lessons and a practical scenario, taken from the first report of the crime through to the preparation of the case for court. The presentations complement the learning created during the practical scenario. The scenario was time specific and will require updating to make it relevant to the period of time in which it is being delivered. It may also be adapted so that the victim company resides in the country in which the course is delivered, in order to make the criminal and procedural legislation more relevant.

1. How to use the trainers guide

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

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.

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

The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching. As such a detailed scenario was created using the timeline that was relevant to the first delivery of this course. In addition, a series of bank accounts were created as supporting material. These use genuine banks and branches to allow students to again use online resources to map the withdrawal of funds to support their investigation. The purpose is to create an awareness of the ability to conduct investigations using online resources as well as using the international cooperation mechanisms that often take far too long to be completed. In order for the supporting materials to be effective in the future, they will need to be updated on a regular basis to make them timely. The current materials are included as a template.

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

Although this course has been developed as a generic, not country specific programme, it is important that trainers personalise their training materials to ensure a more effective delivery of the course material. The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching.

For the 2015 update, the evidence files relate to the potential running of a course in African countries. Specifically, the victim company is located in Mauritius, as this is where the course was expected to be held following the update. Trainers may choose the location of the victim, depending on where the course is being held. It is most likely the victim will be in that country, to enable the complaint to be lodged there. The suspect is located in Germany; however trainers of future courses may wish to locate the suspect in another country, by amending the information. The evidence emails have been recreated in 2015 to make it easier for them to be amended. The file names are neutral, to the extent that they do not include individual names, making the change process less onerous.

1. Course Overview
   1. How long is the course and who is it for

This course is designed as a 3-day programme for judges and prosecutors as part of their initial training programme or in-service programme where they have not had the earlier benefit of this training.

* 1. Who will deliver the course

The course has been developed in order to be delivered by in house trainers within the judicial training centres of countries. Where necessary, it is advisable that subject specialists are introduced to deal with specific technical subjects if the expertise is not available with the judicial centres. For this course it is particularly important to include trainers that have some experience of this type of investigation. To this end it may be appropriate to utilise the knowledge and skills of those from the law enforcement cybercrime community

* 1. How will the course be delivered

The course as currently structured should be delivered in classroom setting using classroom based trainer instruction and practical paper feed exercises. It is recommended that the cohort is divided into working groups of not more than 5 people for the entire course. As detailed above, in Section 1, trainers should consider adapting the exercises and other teaching methods in the programme at the national level. This course is very interactive and will require a great deal of investigation work on the part of the students as well as the provision of high levels of support from the trainers on the course.

* 1. Course objectives

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

**Specific -** Objectives should specify what they want to achieve.

**Measurable** - You should be able to measure whether you are meeting the objectives or not.

**Achievable** - Are the objectives you set, achievable and attainable?

**Realistic -** Can you realistically achieve the objectives with the resources you have?

**Time -** When do you want to achieve the set objectives?

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

* 1. Target students and trainers group

### Students

This course is designed for delivery to judges and prosecutors during their initial training period or during in service training for those that have not taken this course before.

### Experience Prerequisites

This course is designed to be attended only by those that have already completed the introductory cybercrime and electronic evidence, training course, designed by the Council of Europe, or its national equivalent.

### Trainers

Judicial training centres should employ trainers for this course and should include trainers with experience of conducting cybercrime investigations as well as being responsible for the prosecution and adjudication of such cases

### Experience Prerequisites

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

* 1. Resources

### Course Resources requirements

* For delivery of this course in a training room environment, the following equipment is necessary:
* A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group.
* PC/Laptop running Windows 7, 8 or 10 and loaded with MS Office Professional
* Projector and display screen
* Internet access (if available)
* Copies of the Council of Europe Electronic Evidence Guide, version 2
* Whiteboard for each workgroup
* Whiteboard pens (at least 2 each of blue, black, red and green) for each work group
* A Flipchart with adequate paper for each work group
* Student notepaper and pens
* Stapler, hole punch and scissors for each work group
* Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group
* One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken.
* Virtual Machine prepared specifically for this course and included in the resource pack.
* All supporting materials provided with the training pack.

The following resources have been prepared to support the delivery of the course. They are provided in electronic form, as they are voluminous. The COE will provide all resources to countries.

The main information about the scenario and the timescales to be used during the course have been provided in one file that sets out the activities and the key points of the scenario. This file is called 201508 Scenario and evidence for advanced course.doc and is to be found in the resource pack in the Profiles directory.

The following is a list of the files that are to be used in the first practical session 1.1.4. They should be given as a paper feed following an explanation of the scenario. As can be seen, the file name contains the date of the email, it’s order in the sequence and a description. It is important to remember that in the first instance, only the emails without headers should be given as the students should recognise the need for extended headers and ask for them.

|  |
| --- |
| **\Evidence files\Extortion emails** |
| 201508 - Email 1 - suspect to victim extortion email - no headers.docx |
| 201508 - Email 2 - suspect to victim extortion email - no headers.docx |
| 201508 - Email 2 - suspect to victim extortion email- headers.docx |
| 201508 - Email 3 - Humor to suspect - We cannot pay criminals email - no headers.docx |
| 201508 - Email 4 - suspect to victim - instruction email and attachments - headers.docx |
| 201508 - Email 4 - suspect to victim - instruction email and attachments - no headers.docx |
| 201508 - Email 4 - attachment car-original.jpg |
| 201508 - Email 5 - victim to suspect querying instructions for advertising car- no headers.docx |
| 201508 - Email 6 - suspect to victim - Apologies - no headers.docx |
| 201508 - Email 7 - Advert Placed - no headers.docx |
| 201508 - Email 8 - rg realestate to victim - Mercedes Advert has expired |
| 201508 - Email 6 - suspect to victim - Apologies - headers.docx |

The following files relate to the bank accounts that Humor was required to create by the extortionist. They are all HSBC accounts and were used to withdraw the proceeds of the crime from ATM’s in various countries, by the mules recruited by Muller. The ATMs used are genuine and exist in each country. The students should use this as part of their investigation, for example by mapping the withdrawals. If the students have not asked this for by session 1.2.3, it should be provided to them.

HSBC Bank Statement for Zambia Mule.pdf

HSBC Bank Statement for Uganda Mule.pdf

HSBC Bank Statement for Tunisia Mule.pdf

HSBC Bank Statement for Tanzania Mule.pdf

HSBC Bank Statement for Swaziland Mule.pdf

HSBC Bank Statement for South Africa Mule.pdf

HSBC Bank Statement for Senegal Mule.pdf

HSBC Bank Statement for Reunion Mule.pdf

HSBC Bank Statement for Nigeria Mule.pdf

HSBC Bank Statement for Namibia Mule.pdf

HSBC Bank Statement for Mozambique Mule.pdf

HSBC Bank Statement for Morocco Mule.pdf

HSBC Bank Statement for Mauritius.pdf

HSBC Bank Statement for Mauritania Mule.pdf

HSBC Bank Statement for Malawi Mule.pdf

HSBC Bank Statement for Madagascar Mule.pdf

HSBC Bank Statement for Kenya Mule.pdf

HSBC Bank Statement for Ghana Mule.pdf

HSBC Bank Statement for Ethiopia Mule.pdf

HSBC Bank Statement for Egypt Mule.pdf

HSBC Bank Statement for Botswana Mule.pdf

HSBC Bank Statement for Angola Mule.pdf

HSBC Bank Statement for Algeria Mule.pdf

Please note that only 9 mules and the suspect are active in each scenario. The suspect can be allocated a country, depending on the location of the training. Additional bank statements have been created to allow for geographical African scenarios. In addition, there are English and French speaking countries included, to enable training in all GLACY project African countries. For courses outside Africa and particularly those that require European mules, the course material developed in 2012 has European and Balkan countries evidence files that could readily be updated.

The emails sent by the suspect to recruit the mules to assist in the withdrawal of the proceeds of the crime are included in the training pack. They fall into 3 categories under the general heading of “Mule Emails”.

The sub-categories are:

* **Invites to Mules from the suspect (nominally Ralph Muller)**

These are the initial emails that Muller sent to his associates from the motorcycle club. Please remember that include not only those that accepted his offer, but those who declined. These should assist the students to assess the culpability of the mules.

|  |
| --- |
| **\Evidence files\Mule emails\Invites to Mules from suspect** |
| Invite from suspect to mule 1 - headers.docx |
| Invite from suspect to mule 1 - no headers.docx |
| Invite from suspect to mule 2 - headers.docx |
| Invite from suspect to mule 2 - no headers.docx |
| Invite from suspect to mule 3 - headers.docx |
| Invite from suspect to mule 3 - no headers.docx |
| Invite from suspect to mule 4 - headers.docx |
| Invite from suspect to mule 4 - no headers.docx |
| Invite from suspect to mule 5 - headers.docx |
| Invite from suspect to mule 5 - no headers.docx |
| Invite from suspect to mule 6 - headers.docx |
| Invite from suspect to mule 6 - no headers.docx |
| Invite from suspect to mule 7 - headers.docx |
| Invite from suspect to mule 7 - no headers.docx |
| Invite from suspect to mule 8 - headers.docx |
| Invite from suspect to mule 8 - no headers.docx |
| Invite from suspect to mule 9 - headers.docx |
| Invite from suspect to mule 9 - no headers.docx |
| Invite from suspect to mule 10 - headers.docx |
| Invite from suspect to mule 10 - no headers.docx |
| Invite from suspect to mule 11 - headers.docx |
| Invite from suspect to mule 11 - no headers.docx |
| Invite from suspect to mule 12 - headers.docx |
| Invite from suspect to mule 12 - no headers.docx |
| Invite from suspect to mule 13 - headers.docx |
| Invite from suspect to mule 13 - no headers.docx |
| Invite from suspect to mule 14 - headers.docx |
| Invite from suspect to mule 14 - no headers.docx |
| Invite from suspect to mule 15 - headers.docx |
| Invite from suspect to mule 15 - no headers.docx |
| Invite from suspect to mule 16 - headers.docx |
| Invite from suspect to mule 16 - no headers.docx |
| Invite from suspect to mule 17 - headers.docx |
| Invite from suspect to mule 17 - no headers.docx |
| Invite from suspect to mule 18 - headers.docx |
| Invite from suspect to mule 18 - no headers.docx |
| Invite from suspect to mule 19 - headers.docx |
| Invite from suspect to mule 19 - no headers.docx |
| Invite from suspect to mule 20 - headers.docx |
| Invite from suspect to mule 20 - no headers.docx |
| Invite from suspect to mule 21 - headers.docx |
| Invite from suspect to mule 21 - no headers.docx |
| Invite from suspect to mule 22 - headers.docx |
| Invite from suspect to mule 22 - no headers.docx |
| Invite 2 from suspect to mule 12 - headers.docx |
| Invite 2 from suspect to mule 13 - headers.docx |
| Invite 2 from suspect to mule 14 - headers.docx |
| Invite 2 from suspect to mule 17 - headers.docx |
| Invite 2 from suspect to mule 18 - headers.docx |

* **Replies from Mules to the suspect**

These are the replies, accepting or declining the invitation from the suspect:

|  |
| --- |
| **\Evidence files\Mule emails\Replies from Mules to suspect** |
| Reply to suspect from mule 1.docx |
| Reply to suspect from mule 2.docx |
| Reply to suspect from mule 3.docx |
| Reply to suspect from mule 4.docx |
| Reply to suspect from mule 5.docx |
| Reply to suspect from mule 6.docx |
| Reply to suspect from mule 7.docx |
| Reply to suspect from mule 8.docx |
| Reply to suspect from mule 9.docx |
| Reply to suspect from mule 10.docx |
| Reply to suspect from mule 11.docx |
| Reply to suspect from mule 13.docx |
| Reply to suspect from mule 20.docx |
| Reply to suspect from mule 21.docx |
| Reply to mule 21 - bounced message from suspect.docx |
| Reply to suspects bounced messeage - from mule 21.docx |
| Reply to suspect from mule 22.docx |

* **ATM Instructions to Mules from the suspect**

These are the series of messages sent to those accepting the offer form Muller, giving instructions for the withdrawals.

|  |
| --- |
| **\Evidence files\Mule emails\ATM Instructions to Mules from Suspect** |
| ATM Instructions email - mule 1 - no headers.docx |
| ATM Instructions email - mule 2 - no headers.docx |
| ATM Instructions email - mule 3 - no headers.docx |
| ATM Instructions email - mule 4 - no headers.docx |
| ATM Instructions email - mule 5 - no headers.docx |
| ATM Instructions email - mule 6 - no headers.docx |
| ATM Instructions email - mule 7 - no headers.docx |
| ATM Instructions email - mule 8 - no headers.docx |
| ATM Instructions email - mule 9 - no headers.docx |

* **Emails with headers from Mules**

These are the emails from the mules that have the extended headers and may be used by the trainer to help to explain how emails are traced.

|  |
| --- |
| **\Evidence files\Mule emails\Emails with headers from Mules** |
| mule1.docx |
| mule2.docx |
| mule3.docx |
| mule4.docx |
| mule5.docx |
| mule6.docx |
| mule7.docx |
| mule8.docx |
| mule9.docx |
| mule10.docx |
| mule11.docx |
| mule12.docx |
| mule13.docx |
| mule14.docx |

Additional resources have been provided to assist the trainer with preparing the course for delivery. These fall into the general category of profiles and include background information about the scenario, including information about the victim and the motorcycle club, to which all the mules and the suspect belong. Also provided is the Mule contact list and a list of spare mules for further course development. These lists contain personal information about individuals that may be safely used in scenarios. Importantly, they also contain genuine email addresses that may be accessed and used for the creation of up to date messages for the scenario. These files are in the Profiles directory:

201508 Profile - Humor Products

201508 Exchange Rates for Mule Bank Accounts

201508 Money Mules for Africa Scenario (There are also single files for each mule)

201508 Profile – EPIMCA

201508 scenario date calculations

The scenario has an element involving steganography and in order to assist the trainer, the relevant files are included in the training pack. The files are to be found in a directory entitled `Steganography’ These files are:

car-original.JPG

car-original.png

car-original2.jpg

car-stego-new.png

car-stego.png

Card data for photo.docx

Card stripe information.docx

creditcards.txt

Setup-OpenStego-0.5.2.exe

stego-instruction.png

As detailed above, the scenario is the focal point of this course and is supported by a number of subject relevant presentations. These include not only the slides, but the notes as well, to assist the trainer. The presentations are:

FINAL Presentation - Session 1.1.1 - Course Opening and Introductions FINAL.pptx

FINAL Presentation - Session 1.1.2 - Developing an Investigation Plan FINAL.pptx

FINAL Presentation - Session 1.2.1 - Daily Review FINAL.pptx

FINAL Presentation - Session 1.2.2 - Crypto currencies FINAL.pptx

FINAL Presentation - Session 1.2.4 - International Cooperation FINAL.pptx

FINAL Presentation - Session 1.3.1 - Daily Review FINAL.pptx

FINAL Presentation - Session 1.3.2 - Digital Forensics Parts 1 and 2 FINAL

FINAL Presentation - Session 1.3.3 - Preparing a Case for Court Including Evidence Presentation Methods FINAL

FINAL Presentation - Session 1.3.6 - Course Closure FINAL pptx

Due to the nature of this course and its reliance on a developing scenario, it is vital that the trainers takes sufficient time to make themselves aware of the content of the course and prepares for delivery. As has been mentioned, the initial scenario resources were developed in 2012, with the update taking place in 2015. It may be necessary to update some of the messages and bank statements in particular, to make them relevant to the time period in which the course is being delivered. It is the responsibility of the trainer, in conjunction with the training organisation commissioning the course, to ensure its relevance to the audience.

### Course Resources customisation

In order make adapting the complex scenario to country specific needs easier it is possible to use a "search and replace" mechanism that has prepared. Using this functionality it is possible to change not only the dates of the scenario but also the names and other details of the persons involved in the scenario.

The core of the "search and replace" mechanism is a spreadsheet that can be found at the following location:

**\Evidence Files\search-replace-list.xlsx**

This spreadsheet consists of five columns. The first one contains all search terms that need to be replaced. The second column contains all the replacement words. The third column is reserved for internal commands and should be left free. The fourth and the fifth column contain data sets of all replacement terms for an African as well as an European scenario.

The following table shows a schematic representation of the contents:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Search terms** | **Replace terms** | ***res.*** | **African scenario**  **data set** | **European scenario**  **data set** |
| [Mule email 1] | example@mail.com |  | tamtes@dts.mg | erik.lous@bbc.co.uk |
| [Suspect Fullname] | John Doe |  | Gilbert Nadal | Ralf Muller |
| ... | ... |  | ... | ... |

The idea behind the central table is that all data should be changed there and this will lead to customised evidence files.

The only thing that is needed in addition to the spreadsheet is a software that is capable of searching and replacing multiple docx files based on a given xlsx spreadsheet. The following software has been tested for that purpose:

"Useful File Utilities" by Replsoft.com

-> http://www.replsoft.com/

in conjunction with the "Batch replacer for MS Word"

-> http://www.replsoft.com/brformsword.html

The following other software solutions have not been tested but seem to be capable of achieving usable results:

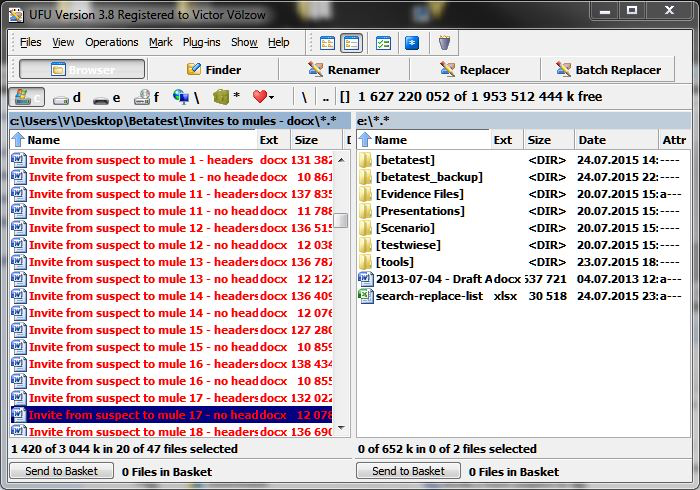
"Find and replace Tool for Word" by Winsometech:

-> http://www.findandreplacetool.com/find-replace-tool-word.html

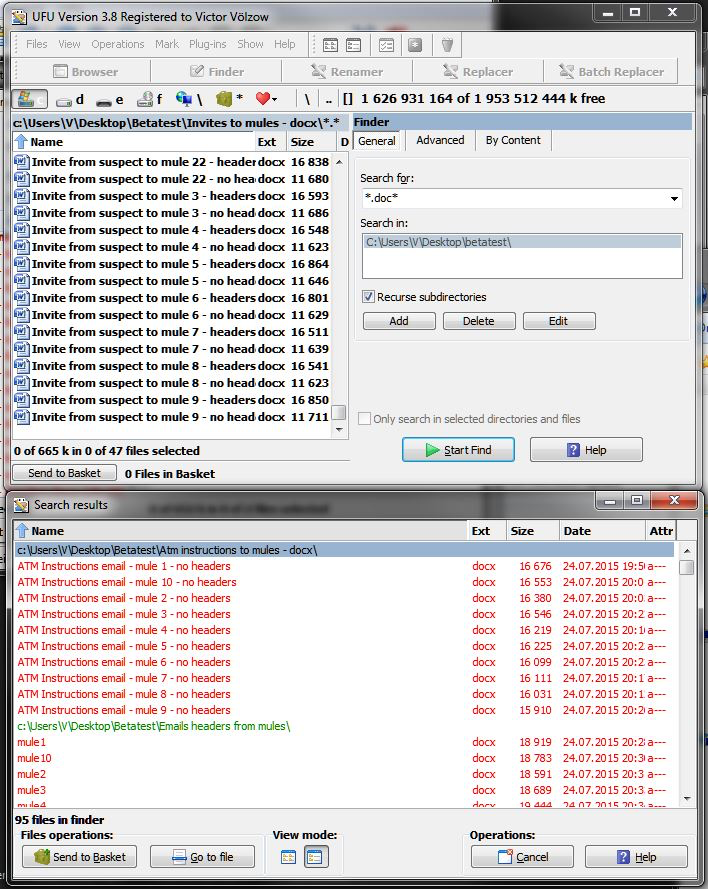
"WordPipe" by Datamystic

-> http://www.datamystic.com/wordpipe

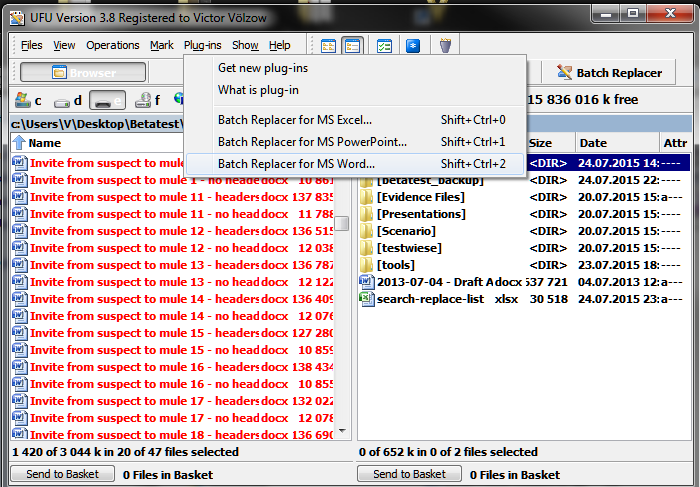
The following screenshots show how the "Useful File Utilities" with the "Batch replacer for MS Word" can be used to search and replace all the search terms from the file "search-replace-list.xlsx".



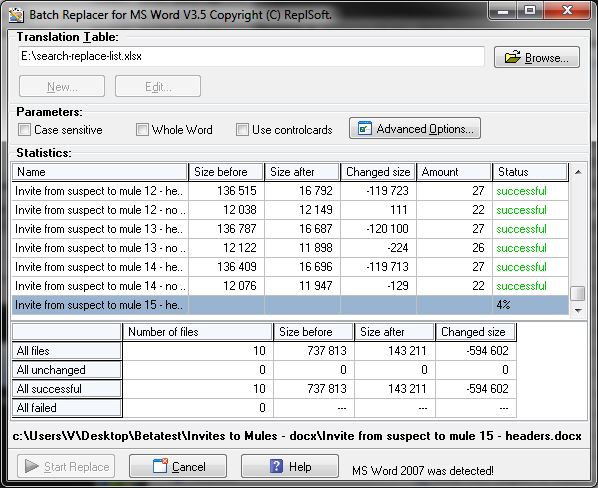
The files that should be progressed need to be selected wither in the "Browser" window or a search for all word documents could be started in the "Finder" window.



The latter option is preferred when all evidence files for the scenario shall be searched and replaced at once.



When the files are selected (indicated by red color) the "Batch Replacer for MS Word" plugin can be started from the "Plug-ins" menu. Of course that plugin needs to be downloaded and installed first (see website above).



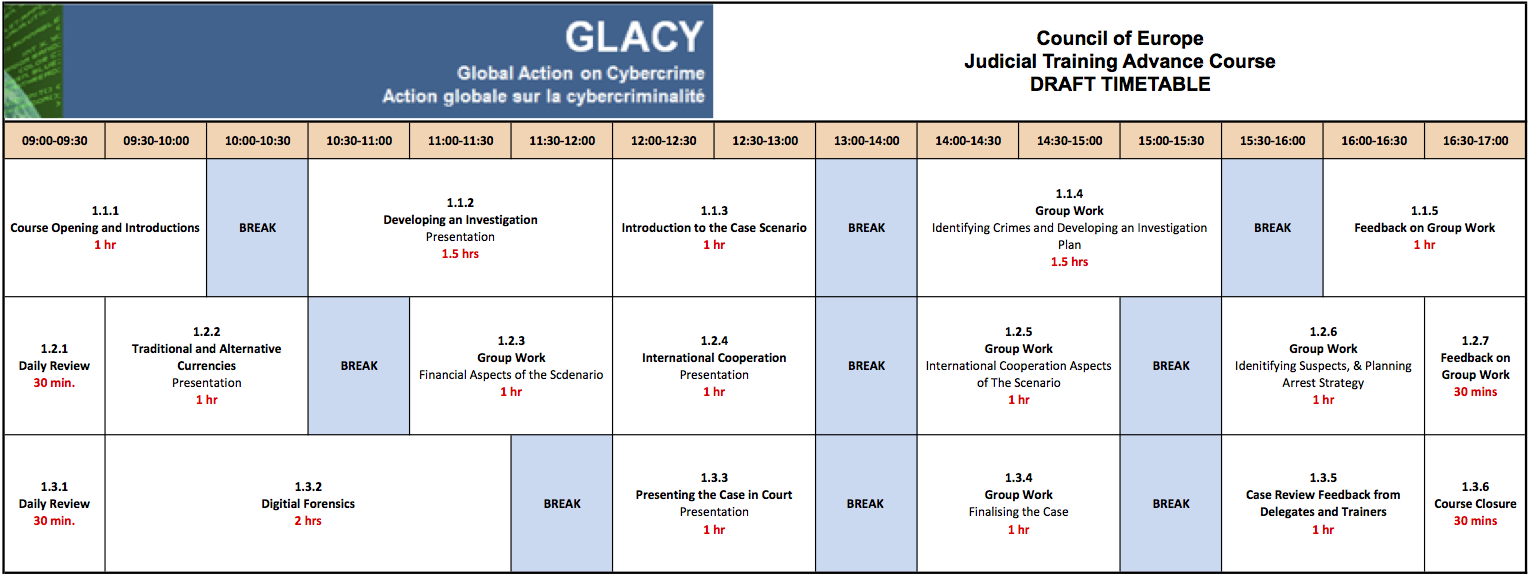
The batch replacer needs to be provided with the "search-replace-list.xlsx" file as translation table. After that the "Start Replace" button at the lower left hand corner can be pressed.

Depending on the system the processing of all the evidence files can take several minutes and even hours.

* 1. Assessment

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

* 1. Timetable



* 1. Course and lesson objectives

|  |  |  |
| --- | --- | --- |
| **Session Number** | **Lesson Title** | **Objectives** |
| **1.1.1** | **Course Introduction** | * Identify the trainers and fellow students * Define course structure and content * Complete relevant administrative tasks * Distribute documentation for course * Introduce the delegates to the trainers and other delegates * Explain facilities and procedures at the venue including Health and Safety Issues |
| **1.1.2** | **Presentation -Developing an Investigation** | * Identify details of the victim * Prepare a short description of the reported facts * Describe the loss, explanation and justification of it * Establish the location of the victim’s computer systems, technical persons responsible with their maintenance who can provide information about them * Discuss the verification and checking conducted by the victim * Assess information of the suspects and possible communication with them * Identify means of communication and the source * Establish the source of criminal activity * Identify the financial instruments involved * Identify witnesses * Consider supporting evidence needed |
| **1.1.2** | **Introducing the Case Scenario** | * Explain the structure scenario links to the presentations of the course * Describe how the presentations relate to the scenario sessions * Explain how the information provided will support the investigation. |
| **1.1.4** | **Group work on the Investigation** | * Identify the crimes committed in the scenario * Develop and investigation plan * Identify further information needed to conduct the investigation * List the resources needed to conduct the investigation |
| **1.1.5** | **Feedback on Group Work** | * Identify the crimes committed in the scenario * Develop and investigation plan * Identify further information needed to conduct the investigation * List the resources needed to conduct the investigation |
| **1.2.1** | **Daily Review** | * Identify areas of the previous days activities that they have understood * Identify such areas where they need to review the materials to bring their knowledge to the required level |
| **1.2.2** | **Presentation – Traditional and Virtual Currencies** | * Explain the term crypto currency * Compare crypto currencies to traditional currencies * Identify different crypto currencies * Outline how crypto currency works * Describe how crypto currency can be used for virtual money laundering * Characterise the challenges that crypto currencies raise for investigations * Describe the possibilities for investigations in crypto currencies. |
| **1.2.3** | **Group work on financial aspects of the scenario** | * Identify the financial trail of the crime proceeds * Identify further information needed to conduct the investigation * List the resources needed to conduct the investigation |
| **1.2.4** | **Presentation -International Cooperation** | * Identify the need for international cooperation for the investigation of many of the offences that may have been committed; * will identify the channels for international cooperation and the available instruments, the ways they are used, the timelines and effectiveness of the methods of cooperation that are available; * will discuss the advantage of the mechanisms of cooperation described within the Budapest Convention on Cybercrime and will identify its general principles, the provisional measures and the 24/7 network. |
| **1.2.5** | **Group work on International Cooperation** | * Apply international cooperation mechanisms to the scenario * Detail the enquiries needed to preserve and obtain evidence from abroad * Develop a plan to acquire evidence from abroad in the most effective manner. * Consider the implications for the investigation of delays in the international cooperation mechanisms |
| **1.2.6** | **Group work identifying the suspect and plan an arrest strategy** | * Consider the evidence provided * Identify the suspects in the case * Identify the witnesses in the case * Develop an arrest strategy for the suspects * Identify the evidence recovery issues * Prepare for the arrest and search of suspect premises * Prepare international requests to support the arrest strategy. |
| **1.2.7** | **Feedback on Group Work** | * Identify the suspect(s) in the scenario * Finalise their investigation plan * Prepare any international requests for assistance. * List the resources needed to conclude the investigation |
| **1.3.1** | **Day 2 Review** | * Identify areas of the previous days activities that they have understood * Identify such areas where they need to review the materials to bring their knowledge to the required level |
| **1.3.2** | **Presentation - Digital Forensics** | * Explain the term Digital Forensics * Compare Digital Forensics to traditional forensic sciences * Define at least three sub-branches of Digital Forensics * Identify the four steps in Digital Forensics examinations * Differentiate the two categories of digital traces * Describe how Digital Forensics can support investigations * Outline how Steganography works * Compare three methods of how to recover deleted files * Characterise different types of Slack Space * Apply Digital Forensics theory to a practical scenario * Identify the benefits of Digital Forensics examination * Describe how Virtualisation can help Digital Forensics |
| **1.3.3** | **Presentation - Preparing the case for court** | * Manage prosecutions * Gather evidence from abroad via MLA's * Ensure that there are no legal or procedural impediments to the requests for evidence * Deal with witnesses in other jurisdictions during the proceedings * Accurately complete or update all relevant documentation and procedures * Ensure that appropriate files and supporting documents are prepared, and present them in the required format within relevant time limits * Disclose evidence to the defence (if needed) * Deal with admissibility of electronic and other evidence * Ensure compliance with ECHR and other provisions are complied with * Know the role and expectations of expert witnesses * Fully document all decisions, actions, options and rationale in accordance with current policy and legislation * Identify methods of presenting electronic evidence in court proceedings |
| **1.3.4** | **Group work on Finalising the Case** | * Prepare the case file for prosecuting the suspect * Consider how digital evidence will be presented in court. * Consider whether digital evidence will require expert evidence. * Finalise the investigation * Establish any gaps in the evidence that may exist |
| **1.3.5** | **Case Review – Feedback from Delegates and Trainers** | * Discuss the outcome of the scenario and the steps taken in the investigation. * Provide feedback on the scenario and its effectiveness |
| **1.3.6** | **Course Closure** | * Provide appropriate feedback on the course and its effectiveness * Complete the course evaluation forms * Identify the next level of learning that they need to undertake to improve their knowledge and skills in the subject matter. |

1. Key Contacts

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

|  |
| --- |
| Alexander Seger  Head of Data Protection & Cybercrime Division  Directorate General of Human Rights and Rule of Law (DG-I)  Council of Europe,  F-67075 Strasbourg Cedex  Tel. +33 3 88 41 21 03  Fax +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int) |

1. Lesson Plans

|  |  |
| --- | --- |
| Lesson: 1.1.1 – Course Opening and Introductions | **Duration: 60 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Computer hardware examples (if available) * Whiteboard * Whiteboard pens (at least 2 each of blue, black, red and green) * 2 Flipcharts with adequate paper * Student notepaper and pens * Stapler, hole punch and scissors * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily | |
| **Aim:** To provide the delegates with information about the need for the training course and its aim and objectives. To ensure that they have sufficient information about the programme of activities and the timetable. Provide information about the health, safety and administrative details of the course. Introduce the delegates to the trainers and other delegates. | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Identify the trainers and fellow delegates * Discuss the overall aim of the course * Explain why this course is necessary * List the component parts of the timetable and activities of the course * List the health and safety procedures for the venue | |
| **Introduction**  This is the opening session of the course. During this session the delegates will be introduced to the trainers and the other delegates. The course aim and objectives will be explained along with the methods of teaching.  The trainer may choose to introduce “ice breakers” to encourage the delegates to become involved in the course and with each other at an early stage.  All information about this session is included in the PowerPoint presentation entitled “Session 1.1.1 – Course Opening and Introductions FINAL” 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**  The only practical exercise in this session is the introduction of the delegates and trainers. This should be conducted in a structured manner, where students introduce each other in pairs. This helps to break the ice at the beginning of the course | |

|  |  |
| --- | --- |
| Lesson: 1.1.2 – Developing an Investigation Plan | **Duration: 90 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * PowerPoint Presentation | |
| **Aim:** The aim of this session is to introduce the delegates to the concept of structured investigations and deals with the relevant elements to be considered from the receipt of the complaint through the investigation. | |
| **Objectives:**   * Identify details of the victim * Prepare a short description of the reported facts * Describe the loss, explanation and justification of it * Establish the location of the victim’s computer systems, technical persons responsible with their maintenance who can provide information about them * Discuss the verification and checking conducted by the victim * Assess information of the suspects and possible communication with them * Identify means of communication and the source * Establish the source of criminal activity * Identify the financial instruments involved * Identify witnesses * Consider supporting evidence needed | |
| **Introduction**  This session provides some useful information about the conduct of investigations. Depending on the legal systems of the delegate countries, they will have differing levels of experience in conducting investigations.  All information about this session is included in the PowerPoint presentation entitled “Session 1.1.2 - Developing an Investigation Plan FINAL” 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 (if applicable)**  There are no practical exercises associated with this session | |

|  |  |
| --- | --- |
| Lesson: 1.1.3 – Introduction to the Case Scenario | **Duration: 60 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * These resources are only needed if the trainer is using a PowerPoint presentation | |
| **Aim:** To provide the delegates with information about the way the case scenario will be introduced into the structure of the course. | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the structure scenario links to the presentations of the course * Describe how the presentations relate to the scenario sessions * Explain how the information provided will support the investigation. | |
| **Introduction:**  This session introduces the scenario to the delegates and provides them with the first documents provided by the victim of the crime, as well as other supporting documents.  The scenario is based on the following background concept that is provided to assist the trainers in understanding the facts:  Humor Products (Humor) is a Hungarian based company that sells expensive car parts on a global basis via the Internet. It has offices in many countries, including Mauritius. Its turnover is €10million per annum and it is a very fast growing business with revenue increasing on an annual basis at a rate of 250%. Humor relies on the Internet for over 85% of its sales. Any interruption to the on line sales capability would have a serious effect on the viability of the business. Humor has just invested €5million in a new storage and distribution warehouse and has taken on a further 20 staff to cope with demand. Unfortunately, as with many fast growing business, disaster recover procedures have not kept pace with the growth in sales and they have no disaster recovery or business continuity plans in place. There is no back up facility that will allow the business to continue in the event of a failure in Internet connectivity.  Ralph Muller is a German citizen who is a self employed IT specialist. He is not faring well in business and is struggling to pay his mortgage and is in debt to his bank. He has several other creditors who are pursuing him for monies owed. In May 2015 he took a Rhine Cruise that was arranged by an international motor cycling club that he belongs to. During the cruise he became friends with a number of people from across Europe, all of whom were members of the motorcycle club. (9 of these people would later become mules in his criminal activities against Humor). Another guest on the trip was Veselko Ivanković who is the IT director of Humor, currently working in Mauritius on the Humor network servers, based in Port Louis. The servers support the entire Humor infrastructure. Veselko and Ralph became good friends on the trip. Veselko was disillusioned with his job and was very indiscreet in his discussions with Ralph, explaining that his employers did not understand anything about IT security and that their business not survive an attack on its systems. There is no suggestion that Veselko was in any way involved in the events that later occurred.  Ralph Muller returned home after the holiday to be met by a large pile of letters demanding immediate repayment of his debts. He decided that he would take advantage of the information he received from Veselko on holiday and then set out a plan to extort money from Humor.  Muller devises a plan to extort money from Humor and an email exchange occurs in which he finally achieves his objective and persuades Humor to follow a circuitous route to pass the money to him. In turn he uses a series of money mules, in different countries to collect money from ATM’s, having provided them with cards to do so. The entire story is in the emails and these support the course. In addition, there are bank statements that show the withdrawals, as well as lists of the mules. All players in this scenario have genuine email addresses. The user names and passwords are in the lists provided with the pack and can be used if it is deemed necessary to recreate the scenario to make sure the dates on the emails and in the bank statements are in a relevant time period to the course delivery. The bank statements show withdrawals of the money over a period of time. The ATM’s used are genuine and could, if the students consider it, be mapped to show the area in which the various withdrawals were made. Once again, it may be necessary to update the bank statements to make them date relevant. There is no single solution to this scenario and the purpose is to enable the students to consider the various options and identify what evidence is needed and how to get it, both for the investigation and the court proceedings. The trainers will need to be very interactive and provide support for the students; in some circumstances, it may be necessary to provide additional assistance to ensure the timetable is adhered to and the results are achieved.  **Information for delegates**  The following is the profile of the victim company, Humor Products.  Humor Products (Humor) is a Hungarian based company that sells expensive car parts on a global basis via the Internet. It has offices in many countries, including Mauritius, where its servers are based that support its entire infrastructure. Its turnover is €10million per annum and it is a very fast growing business with revenue increasing on an annual basis at a rate of 250%. Humor relies on the Internet for over 85% of its sales. Any interruption to the on line sales capability would have a serious effect on the viability of the business. Humor has just invested €5million in a new storage and distribution warehouse and has taken on a further 20 staff to cope with demand. Unfortunately, as with many fast growing business, disaster recover procedures have not kept pace with the growth in sales and they have no disaster recovery or business continuity plans in place. There is no back up facility that will allow the business to continue in the event of a failure in Internet connectivity.  The CEO and director of Humor is Ratimir Novosel who took over the company from his father in 2004. He has been responsible for its rapid development since that date. The management structure in the company has not developed at the same pace as the business activity. Humor has been somewhat overwhelmed by the success of their online business.  Vaselko Ivankovic, who has been with the company for 5 years, manages the IT systems and online presence. He is responsible for the management of the systems as well as the security aspects of the online business. He has been making representation to the CEO for upwards of 2 years to the effect that the security of the company servers requires a security overhaul. The CEO has been too busy developing the business to act on these warnings.  **Contact details:**  Humor Products  7782 Sárok  Piroska u. 23. Hungary  **Phone:**(69) 912-707  **Email:** [humorproducts@gmail.com](mailto:humorproducts@gmail.com)  **Creation Date:** 1st January 1960  **Mauritius Contact Details**  Humor Products  Address : 9th Floor, Sir William Newton Street,  Port-Louis, Mauritius  Phone : (230) 211-6314  A printable file named ‘201508 Profile - Humor Products’ is in the profiles subdirectory of the course materials.  The following files contain the initial email trail that was sent to the victim by the offender and the responses. These should be given to the students for them to consider:  **\Evidence files\Extortion emails**  201508 - Email 1 - suspect to victim extortion email - no headers.docx  201508 - Email 2 - suspect to victim extortion email - no headers.docx  201508 - Email 3 - Humor to suspect - We cannot pay criminals email - no headers.docx  201508 - Email 4 - suspect to victim - instruction email and attachments - no headers.docx  201508 - Email 4 - attachment car-original.jpg  201508 - Email 5 - victim to suspect querying instructions for advertising car- no headers.docx  201508 - Email 6 - suspect to victim - Apologies - no headers.docx  201508 - Email 7 - Advert Placed - no headers.docx  201508 - Email 8 - rg realestate to victim - Mercedes Advert has expired  The following files contains the same email and with extended headers. They should be given to the students when they request the extended headers:  201508 - Email 2 - suspect to victim extortion email- headers.docx  201508 - Email 4 - suspect to victim - instruction email and attachments - headers.docx  201508 - Email 6 - suspect to victim - Apologies - headers.docx  If the students reach the conclusion that they need the bank statements of Humor products to conduct their investigation. Some of the following files should be provided. Only the accounts that relate to the specific mules used on the course should be provided. The others are standby files for use on other courses. Please note that the dates should be amended to reflect the period when the course will run.  HSBC Bank Statement for Zambia Mule.pdf  HSBC Bank Statement for Uganda Mule.pdf  HSBC Bank Statement for Tunisia Mule.pdf  HSBC Bank Statement for Tanzania Mule.pdf  HSBC Bank Statement for Swaziland Mule.pdf  HSBC Bank Statement for South Africa Mule.pdf  HSBC Bank Statement for Senegal Mule.pdf  HSBC Bank Statement for Reunion Mule.pdf  HSBC Bank Statement for Nigeria Mule.pdf  HSBC Bank Statement for Namibia Mule.pdf  HSBC Bank Statement for Mozambique Mule.pdf  HSBC Bank Statement for Morocco Mule.pdf  HSBC Bank Statement for Mauritius.pdf  HSBC Bank Statement for Mauritania Mule.pdf  HSBC Bank Statement for Malawi Mule.pdf  HSBC Bank Statement for Madagascar Mule.pdf  HSBC Bank Statement for Kenya Mule.pdf  HSBC Bank Statement for Ghana Mule.pdf  HSBC Bank Statement for Ethiopia Mule.pdf  HSBC Bank Statement for Egypt Mule.pdf  HSBC Bank Statement for Botswana Mule.pdf  HSBC Bank Statement for Angola Mule.pdf  HSBC Bank Statement for Algeria Mule.pdf  Information about the mules is contained in the following file, with individual files for each mule also available. ‘201508 Money Mules for Africa Scenario.doc’, which is in the Profiles directory of the course materials  The course developer and trainers should ensure that they have read and are familiar with the emails and other documents in order that the delivery of the course is effective.  The scenario is straightforward; however it is designed so that the students should identify the items that they will need to conduct the investigation. It is essential to aid the learning that they are provided with minimal information to begin with and then other evidence as and when they identify its existence. For example, the emails without headers should be given at first and the students can then ask for additional information, such as the extended headers. | |

|  |  |
| --- | --- |
| Lesson: 1.1.4 – Group Work – Identifying Crimes | **Duration: 90 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is the opening of the practical scenario. The aim is for the delegates to identify roles in the investigation team, allocate tasks, and identify the parameters of the investigation to be conducted as well as the offences that may have been committed. | |
| **Objectives:**  At the end of this session the student will be able to:   * Identify the crimes committed in the scenario * Develop and investigation plan * Identify further information needed to conduct the investigation * List the resources needed to conduct the investigation | |
| **Introduction:**  The use of a presentation is optional for this session. If necessary a presentation may be used to support the paper feed exercise that provides the students with sufficient information to commence an investigation and meet the objectives of the session. | |
| **Practical Exercises (if applicable):** This session is entirely practical and begins with the examination of the documents provided that supports the complaint by the victim of the crime. Trainers should support the delegates through out the practical sessions of the course, to ensure they are following the correct leads as well as assisting them and evaluating their performance. | |

|  |  |
| --- | --- |
| Lesson: 1.1.5 – Feedback on Group Work | **Duration: 60 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is to ensure that the delegates have understood the scenario and acted upon the evidence provided to them, to identify crimes under investigations and have developed their investigation plan. | |
| **Objectives:**  At the end of this session the student will be able to:   * Identify the crimes committed in the scenario * Develop an investigation plan * Identify further information needed to conduct the investigation * List the resources needed to conduct the investigation | |
| **Introduction:**  The use of a presentation is optional for this session. If necessary a presentation may be used to support the paper feed exercise that provides the students with sufficient information to commence an investigation and meet the objectives of the session. | |
| **Practical Exercises (if applicable):** This is a practical session from the perspective that delegates will be asked to explain the result of their investigations and explain how the investigation will continue. They will be expected to identify next lines of enquiry and what support they will need. | |

|  |  |
| --- | --- |
| Lesson: 1.2.1 – Daily Review | **Duration: 30 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * PowerPoint Presentation | |
| **Aim:**  The purpose of this session is to review the previous days activities, obtain feedback from the delegates and check that the objectives of the sessions have been met | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Identify areas of the previous days activities that they have understood * Identify such areas where they need to review the materials to bring their knowledge to the required level | |
| **Introduction**  This session has been prepared to allow students to check that they have understood the previous days teaching and that they are able to meet each of the objectives for the individual sessions. It is also to provide the trainer the opportunity to check the knowledge level of the students and to identify areas where the teaching materials may be improved.  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.2.1 - Daily Review FINAL’ 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. | |

|  |  |
| --- | --- |
| Lesson: 1.2.2 – Traditional and Alternative Currencies | **Duration: 60 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * PowerPoint Presentation | |
| **Aim:**  The purpose of this session is to introduce the delegates to the concept of virtual currencies and how they may impact on investigations | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the term crypto currency * Compare crypto currencies to traditional currencies * Identify different crypto currencies * Outline how crypto currency works * Describe how crypto currency can be used for virtual money laundering * Characterise the challenges that crypto currencies raise for investigations * Describe the possibilities for investigations in crytpo currencies. | |
| **Introduction:**  This session has been introduced to the 2015 update of the course to enable the delegates to consider the potential impact of virtual currencies, in the context of use by criminals and the impact on investigations.  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.2.2. - Crypto currencies FINAL’ 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. | |

|  |  |
| --- | --- |
| Lesson: 1.2.3 – Group Work – Financial Aspects | **Duration: 90 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is to allow the delegates to consider the financial implications of the scenario and to request bank records that may be relevant. | |
| **Objectives:**  At the end of this session the student will be able to:   * Identify the financial trail of the crime proceeds * Identify further information needed to conduct the investigation * List the resources needed to conduct the investigation | |
| **Introduction:**  The use of a presentation is optional for this session. If necessary a presentation may be used to support the paper feed exercise that provides the students with sufficient information to commence an investigation and meet the objectives of the session. If not asked for by now, the following files should be provided to the delegates at the beginning of this session:  HSBC Bank Statement for Zambia Mule.pdf  HSBC Bank Statement for Uganda Mule.pdf  HSBC Bank Statement for Tunisia Mule.pdf  HSBC Bank Statement for Tanzania Mule.pdf  HSBC Bank Statement for Swaziland Mule.pdf  HSBC Bank Statement for South Africa Mule.pdf  HSBC Bank Statement for Senegal Mule.pdf  HSBC Bank Statement for Reunion Mule.pdf  HSBC Bank Statement for Nigeria Mule.pdf  HSBC Bank Statement for Namibia Mule.pdf  HSBC Bank Statement for Mozambique Mule.pdf  HSBC Bank Statement for Morocco Mule.pdf  HSBC Bank Statement for Mauritius.pdf  HSBC Bank Statement for Mauritania Mule.pdf  HSBC Bank Statement for Malawi Mule.pdf  HSBC Bank Statement for Madagascar Mule.pdf  HSBC Bank Statement for Kenya Mule.pdf  HSBC Bank Statement for Ghana Mule.pdf  HSBC Bank Statement for Ethiopia Mule.pdf  HSBC Bank Statement for Egypt Mule.pdf  HSBC Bank Statement for Botswana Mule.pdf  HSBC Bank Statement for Angola Mule.pdf  HSBC Bank Statement for Algeria Mule.pdf | |
| **Practical Exercises (if applicable):** This session is entirely practical and follows from the examination of the documents provided that supports the complaint by the victim of the crime. This session should concentrate on the financial aspects of the crime and in particular the money trail from the HSBC account of Humor Products. Trainers should support the delegates through out the practical sessions of the course, to ensure they are following the correct leads as well as assisting them and evaluating their performance. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.2.4 – Presentation - International Cooperation | **Duration: 60 Minutes** | |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | | |
| **Aim:** This session is to allow the delegates to consider the financial implications of the scenario and to request bank records that may be relevant. | |
| **Objectives:**  At the end of this session the student will be able to:   * Identify the need of international cooperation for the investigation of many of the offences that may have been committed; * Identify the channels for international cooperation and the available instruments, the ways they are used, the timelines and effectiveness of the methods of cooperation that are available; * Discuss the advantage of the mechanisms of cooperation described within the Budapest Convention on Cybercrime and will identify its general principles, the provisional measures and the 24/7 network. | |
| **Introduction:**  This session will underline the importance of international cooperation to the investigation of concrete cases of cybercrimes. International cooperation available instruments, mainly the Budapest Convention on Cybercrime, will be described.  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.2.4 - International cooperation FINAL’ 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. | |

|  |  |
| --- | --- |
| Lesson: 1.2.5 – Group Work – International Cooperation | **Duration: 60 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide version 2 * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is designed to allow students to consider the nature of the international enquiries they will need to conduct on order to obtain the evidence of the crimes they have identified in the investigation planning stage. They should consider the various levels of cooperation available. | |
| **Objectives:**  At the end of this session students will be able to:   * Apply international cooperation mechanisms to the scenario * Detail the enquiries needed to preserve and obtain evidence from abroad * Develop a plan to acquire evidence from abroad in the most effective manner. * Consider the implications for the investigation of delays in the international cooperation mechanisms | |
| **Introduction:**  There is no presentation associated with this session. | |
| **Practical Exercises (if applicable)** Once again, this is a practical session, where the students will consider their investigation plan from the perspective of securing and obtaining evidence related to the scenario. The information provided should already have provided them with sufficient considerations, in terms of preservation of data that is likely to be deleted before and MLAT and the subsequent obtaining of preserved data in evidential form. The presentation in the previous session should be used by the students to prioritise and identify the best methods. | |

|  |  |
| --- | --- |
| Lesson: 1.2.6 – Group Work – Identifying the Suspects | **Duration: 60 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * PC/Laptop running Windows 7 or 8 and loaded with MS Office Professional * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session provides the opportunity for the students to pull together all the evidence they have been given during day one and consider the identity of any suspects in order to develop and arrest and evidence recovery strategy | |
| **Objectives:**  At the end of this session students will be able to:   * Consider the evidence provided * Identify the suspects in the case * Identify the witnesses in the case * Develop an arrest strategy for the suspects * Identify the evidence recovery issues * Prepare for the arrest and search of suspect premises * Prepare international requests to support the arrest strategy. | |
| **Introduction:**  There is no presentation associated with this session. | |
| **Practical Exercises (if applicable)**  This session is the final practical on day two of the course. Students will have compiled all available evidence and will consider the identity of any suspects. They will then develop an arrest and search and seizure strategy as well as identify aspects of international cooperation that are necessary. At the end of the session students should have reached the conclusion that the primary offender for this version of the course, is Ralph Muller. If they have not reached this conclusion, they should receive assistance from the trainer, who should explain how an investigation would reach this conclusion.  The following day’s session rely upon Muller being identified as within the scenario, he will have been arrested by the start of day 3, his computer seized and a forensic examination conducted. This examination will form the 2nd part of the digital forensics presentation on day 3. | |

|  |  |
| --- | --- |
| Lesson: 1.2.7 – Feedback on Group Work | **Duration: 60 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is to ensure that the delegates have understood the scenario and acted upon the evidence provided to them, to identify the money flow and the identity of the suspect(s). They should have a plan to arrest the suspect and recover evidence of the crimes. | |
| **Objectives:**  At the end of this session the student will be able to:   * Identify the suspect(s) in the scenario * Finalise their investigation plan * Prepare any international requests for assistance. * List the resources needed to conclude the investigation | |
| **Introduction:**  The use of a presentation is optional for this session. If necessary a presentation may be used to support the paper feed exercise that provides the students with sufficient information to commence an investigation and meet the objectives of the session. | |
| **Practical Exercises (if applicable):** This is a practical session from the perspective that delegates will be asked to explain the result of their investigations and explain how the investigation will continue. They will be expected to identify next lines of enquiry and what support they will need. | |

|  |  |
| --- | --- |
| Lesson: 1.3.1 – Daily Review | **Duration: 30 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * PowerPoint Presentation | |
| **Aim:**  The purpose of this session is to review the previous days activities, obtain feedback from the delegates and check that the objectives of the sessions have been met | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Identify areas of the previous days activities that they have understood * Identify such areas where they need to review the materials to bring their knowledge to the required level | |
| **Introduction**  This session has been prepared to allow students to check that they have understood the previous days teaching and that they are able to meet each of the objectives for the individual sessions. It is also to provide the trainer the opportunity to check the knowledge level of the students and to identify areas where the teaching materials may be improved.  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.3.1 - Daily Review FINAL’ 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. | |

|  |  |
| --- | --- |
| Lesson: 1.3.2 – Presentation – Digital Forensics | **Duration: 120 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * PowerPoint Presentation | |
| **Aim:** The aim of this session is to raise the awareness of the delegates in respect of the science of digital forensics and its value to criminal investigations. It also provides information about the evidence found in relation to the scenario. | |
| **Objectives:**  At the end of this session participants will be able to:   * Explain the term Digital Forensics * Compare Digital Forensics to traditional forensic sciences * Define at least three sub-branches of Digital Forensics * Identify the four steps in Digital Forensics examinations * Differentiate the two categories of digital traces * Describe how Digital Forensics can support investigations * Outline how Steganography works * Compare three methods of how to recover deleted files * Characterise different types of Slack Space * Apply Digital Forensics theory to a practical scenario * Identify the benefits of Digital Forensics examination * Describe how Virtualisation can help Digital Forensics | |
| **Introduction:**  This session is divided into two parts, firstly background on the value of the digital forensics in criminal investigations, and secondly a presentation on the digital evidence in the case scenario.  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.3.2 - Digital Forensics Parts 1 and 2 FINAL’ 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 (if applicable)** There are no practical exercises in this session; however there are demonstrations by the trainer. | |

|  |  |
| --- | --- |
| Lesson: 1.2.3 – Group Work – Digital Forensics | **Duration: 90 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 6 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is to allow the students to consider the implications of digital evidence in the context of what has been found on the computer of the suspect. They will also consider what other evidence is now needed. | |
| **Objectives:**  **At the end of this session, the students will be able to:**   * Identify the evidence that is required to be produced from the suspect computer * Establish what other enquiries are needed to support this evidence * Consider the criminal culpability of others involved in the scenario | |
| **Introduction:**  This session is entirely practical does not contain a presentation | |
| **Practical Exercises (if applicable)** The following files are the exchange of emails between the offender and the mules. These are found on the computer of the suspect after arrest. They should be provided to the students to allow them to continue the investigation and to consider the culpability of the mules as well as the extent of the evidence they will need from abroad.  There are other mules that to which the suspect sent a request for assistance. These mules did not engage in the illegal activity but may still be witnesses. The personal details in the file may be used to create email accounts and to use those that were created for the scenario. | |

|  |  |
| --- | --- |
| Lesson: 1.2.4 – Presentation – Preparing the Case for Court | **Duration: 60 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * PowerPoint Presentation | |
| **Aim:** This session is aimed at providing the students with sufficient information to allow them to make decisions about how the case will be prepared and presented to the court, considering all the options and issues that may be pertinent to the court itself | |
| **Objectives:**  At the end of this session participants will be able to:   * Manage prosecutions * Gather evidence from abroad via MLA's * Ensure that there are no legal or procedural impediments to the requests for evidence * Deal with witnesses in other jurisdictions during the proceedings * Accurately complete or update all relevant documentation and procedures * Ensure that appropriate files and supporting documents are prepared, and present them in the required format within relevant time limits * Disclose evidence to the defence (if needed) * Deal with admissibility of electronic and other evidence * Ensure compliance with ECHR and other provisions are complied with * Know the role and expectations of expert witnesses * Fully document all decisions, actions, options and rationale in accordance with current policy and legislation * Identify methods of presenting electronic evidence in court proceedings | |
| **Introduction:**  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.3.3 - Preparing a Case for Court Including Evidence Presentation Methods FINAL’ 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 (if applicable)** There are no practical exercises in this session. | |

|  |  |
| --- | --- |
| Lesson: 1.3.4 – Group Work – Finalising the Case | **Duration: 60 Minutes** |
| **Resources required:**   * A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 6 students per group. * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Internet access (if available) * Copies of the Council of Europe Electronic Evidence Guide version 2 * Whiteboard for each workgroup * Whiteboard pens (at least 2 each of blue, black, red and green) for each work group * A Flipchart with adequate paper for each work group * Student notepaper and pens * Stapler, hole punch and scissors for each work group * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily per work group * One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken. * All supporting materials provided with the training pack. | |
| **Aim:** This session is designed to allow the students to pull together all the evidence in a manner, which will produce a compelling case against the defendants. They will examine the admissibility of all evidence collected as well as ensuring that it has all be obtained in accordance with national and international laws and good practice. | |
| **Objectives:**  At the end of this session participants will be able to:   * Consider all aspects in the management of prosecutions * Ensure the integrity of evidence received from abroad. * Establish there are no impediments to the admissibility of evidence obtained * Deal with witnesses in other jurisdictions during the proceedings * Ensure compliance with ECHR and other provisions are complied with | |
| **Introduction**  There is no presentation associated with this session | |
| **Practical Exercises (if applicable)**  This session is entirely practical in nature and the teams will work together will all the evidence that has been obtained to prepare a case file for presentation to the training team. The trainer should ensure that the students take account of all the evidence and identify any outstanding issues that would require attention.  All the evidence should be made available to the students during this session, even if they did not identify some parts of it during their investigation. Depending on the time available each team should produce a short report detailing their findings. In any event, each team should give a presentation to the others, detailing the key issues and any lessons learned as a result of the practical exercises. | |

|  |  |
| --- | --- |
| Lesson: 1.2.5 – Case Review – Feedback | **Duration 60 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector * Delegate evaluation forms | |
| **Aim:**  This session is designed to allow the delegates to present their findings on the case scenario and for the trainers and delegates to provide feedback on the activities and findngs. | |
| **Objectives:**  At the end of this session participants will be able to:   * Provide appropriate feedback on the scenario and its effectiveness * Identify the next level of learning that they need to undertake to improve their knowledge and skills in the subject matter. | |
| **Introduction**  This is an important session of the course and should be used to obtain feedback from the students on the case scenario and methodology used to deliver the course. | |
| **Practical Exercises (if applicable)** There are no practical exercises in this session. | |

|  |  |
| --- | --- |
| Lesson: 1.3.6 – Course Closure | **Duration 30 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7 and with Office 2010 * Projector * PowerPoint Presentation * Delegate evaluation forms | |
| **Aim:**  This session is designed to allow the delegates to provide feedback on the course and to assist the trainer in identifying any improvements that may be made. It is also for the trainer to recap on the contents of the course by reference to the aim and objectives. | |
| **Objectives:**  At the end of this session participants will be able to:   * Provide appropriate feedback on the course and its effectiveness * Complete the COE course evaluation forms * Identify the next level of learning that they need to undertake to improve their knowledge and skills in the subject matter. | |
| **Introduction**  This is an important session of the course and should be used to obtain feedback from the students on the course content and methodology used to deliver the course. Any evaluation forms should be completed or finalised during this session. The trainer should recap on all the session of the course and check that the objectives have been met. Once the session is over the trainer is responsible for ensuring that all feedback in considered and that any changes that are necessary, are implemented in the course either as an ongoing minor modification or during a scheduled major modification update.  All information about this session is included in the PowerPoint presentation entitled ‘Session 1.3.6 - Course Closure FINAL’ 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 (if applicable)** There are no practical exercises in this session. | |

1. Evaluation

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

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

An evaluation from has been prepared and is provided as a template to be adapted to local conditions. Trainers are responsible for ensuring that the forms are completed and returned to the relevant national body in order that improvements may be made for further delivery of the course.

1. Assessment

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

**Appendices**

**Training Materials**

The following list is the supporting materials for the course. The Header box gives information about the location of the files in the directory structure. Information about when to use the files appears in the relevant Session number above.

|  |
| --- |
| **\Presentations** |
| FINAL Presentation - Session 1.1.1 - Course Opening and Introductions FINAL.pptx |
| FINAL Presentation - Session 1.1.2 - Developing an Investigation Plan FINAL.pptx |
| FINAL Presentation - Session 1.2.1 - Daily Review FINAL.pptx |
| FINAL Presentation - Session 1.2.2 - Crypto currencies FINAL.pptx |
| FINAL Presentation - Session 1.2.4 - International Cooperation FINAL.pptx |
| FINAL Presentation - Session 1.3.1 - Daily Review FINAL.pptx |
| FINAL Presentation - Session 1.3.2 - Digital Forensics Parts 1 and 2 FINAL |
| FINAL Presentation - Session 1.3.3 - Preparing a Case for Court Including Evidence Presentation Methods FINAL |
| FINAL Presentation - Session 1.3.6 - Course Closure FINAL pptx |

|  |
| --- |
| **\Profiles** |
| 201508 Scenario and evidence for advanced course |
| 201508 Exchange Rates for Mule Bank Accounts |
| 201508 Money Mules for Africa Scenario |
| 201508 Profile - Humor Products |
| 201508 Profile - EPIMCA |
| 201508 scenario date calculations |

|  |
| --- |
| **\Evidence files\Extortion emails** |
| 201508 - Email 1 - suspect to victim extortion email - no headers.docx |
| 201508 - Email 2 - suspect to victim extortion email - no headers.docx |
| 201508 - Email 2 - suspect to victim extortion email- headers.docx |
| 201508 - Email 3 - Humor to suspect - We cannot pay criminals email - no headers.docx |
| 201508 - Email 4 - suspect to victim - instruction email and attachments - headers.docx |
| 201508 - Email 4 - suspect to victim - instruction email and attachments - no headers.docx |
| 201508 - Email 4 - attachment 387\_237 pixels |
| 201508 - Email 4 - attachment 547\_558 pixels |
| 201508 - Email 4 - attachment car-original |
| 201508 - Email 5 - victim to suspect querying instructions for advertising car- no headers.docx |
| 201508 - Email 6 - suspect to victim - Apologies - no headers.docx |
| 201508 - Email 7 - Advert Placed - no headers.docx |
| 201508 - Email 8 - rg realestate to victim - Mercedes Advert has expired |
| 201508 - Email 6 - suspect to victim - Apologies - headers.docx |

|  |
| --- |
| **\Evidence files\Mule emails\Invites to Mules from suspect** |
| Invite from suspect to mule 1 - headers.docx |
| Invite from suspect to mule 1 - no headers.docx |
| Invite from suspect to mule 2 - headers.docx |
| Invite from suspect to mule 2 - no headers.docx |
| Invite from suspect to mule 3 - headers.docx |
| Invite from suspect to mule 3 - no headers.docx |
| Invite from suspect to mule 4 - headers.docx |
| Invite from suspect to mule 4 - no headers.docx |
| Invite from suspect to mule 5 - headers.docx |
| Invite from suspect to mule 5 - no headers.docx |
| Invite from suspect to mule 6 - headers.docx |
| Invite from suspect to mule 6 - no headers.docx |
| Invite from suspect to mule 7 - headers.docx |
| Invite from suspect to mule 7 - no headers.docx |
| Invite from suspect to mule 8 - headers.docx |
| Invite from suspect to mule 8 - no headers.docx |
| Invite from suspect to mule 9 - headers.docx |
| Invite from suspect to mule 9 - no headers.docx |
| Invite from suspect to mule 10 - headers.docx |
| Invite from suspect to mule 10 - no headers.docx |
| Invite from suspect to mule 11 - headers.docx |
| Invite from suspect to mule 11 - no headers.docx |
| Invite from suspect to mule 12 - headers.docx |
| Invite from suspect to mule 12 - no headers.docx |
| Invite from suspect to mule 13 - headers.docx |
| Invite from suspect to mule 13 - no headers.docx |
| Invite from suspect to mule 14 - headers.docx |
| Invite from suspect to mule 14 - no headers.docx |
| Invite from suspect to mule 15 - headers.docx |
| Invite from suspect to mule 15 - no headers.docx |
| Invite from suspect to mule 16 - headers.docx |
| Invite from suspect to mule 16 - no headers.docx |
| Invite from suspect to mule 17 - headers.docx |
| Invite from suspect to mule 17 - no headers.docx |
| Invite from suspect to mule 18 - headers.docx |
| Invite from suspect to mule 18 - no headers.docx |
| Invite from suspect to mule 19 - headers.docx |
| Invite from suspect to mule 19 - no headers.docx |
| Invite from suspect to mule 20 - headers.docx |
| Invite from suspect to mule 20 - no headers.docx |
| Invite from suspect to mule 21 - headers.docx |
| Invite from suspect to mule 21 - no headers.docx |
| Invite from suspect to mule 22 - headers.docx |
| Invite from suspect to mule 22 - no headers.docx |
| Invite 2 from suspect to mule 10 - headers.docx |
| Invite 2 from suspect to mule 10 - no headers.docx |
| Invite 2 from suspect to mule 11 - headers.docx |
| Invite 2 from suspect to mule 11 - no headers.docx |
| Invite 2 from suspect to mule 12 - headers.docx |
| Invite 2 from suspect to mule 12 - no headers.docx |
| Invite 2 from suspect to mule 13 - headers.docx |
| Invite 2 from suspect to mule 13 - no headers.docx |
| Invite 2 from suspect to mule 14 - headers.docx |
| Invite 2 from suspect to mule 14 - no headers.docx |

|  |
| --- |
| **\Evidence files\Mule emails\Replies from Mules to suspect** |
| Reply to suspect from mule 1 - no headers.docx |
| Reply to suspect from mule 2- no headers.docx |
| Reply to suspect from mule 3 - no headers.docx |
| Reply to suspect from mule 4 - no headers.docx |
| Reply to suspect from mule 5 - no headers.docx |
| Reply to suspect from mule 6 - no headers.docx |
| Reply to suspect from mule 7 - no headers.docx |
| Reply to suspect from mule 8 - no headers.docx |
| Reply to suspect from mule 9 - no headers.docx |
| Reply to suspect from mule 12 - no headers.docx |
| Reply to suspect from mule 15 - no headers.docx |
| Reply to suspect from mule 17 - no headers.docx |
| Reply to suspect - bounced message - from mule 17 - no headers.docx |
| Reply to suspect from mule 19 - no headers.docx |
| Reply to suspect from mule 22 - no headers.docx |

|  |
| --- |
| **\Evidence files\Mule emails\ATM Instructions to Mules from Suspect** |
| ATM Instructions email - mule 1 - no headers.docx |
| ATM Instructions email - mule 2 - no headers.docx |
| ATM Instructions email - mule 3 - no headers.docx |
| ATM Instructions email - mule 4 - no headers.docx |
| ATM Instructions email - mule 5 - no headers.docx |
| ATM Instructions email - mule 6 - no headers.docx |
| ATM Instructions email - mule 7 - no headers.docx |
| ATM Instructions email - mule 8 - no headers.docx |
| ATM Instructions email - mule 9 - no headers.docx |

|  |
| --- |
| **\Evidence files\Mule emails\Emails with headers from Mules** |
| mule1.docx |
| mule2.docx |
| mule3.docx |
| mule4.docx |
| mule5.docx |
| mule6.docx |
| mule7.docx |
| mule8.docx |
| mule9.docx |
| mule10.docx |
| mule11.docx |
| mule12.docx |
| mule13.docx |
| mule14.docx |

|  |
| --- |
| **\Evidence files\Money Mule and ATM information sheets** |
| Countries for Money Mules for Africa Scenario |
| Algeria - Mule and ATM information sheet |
| Angola - Mule and ATM information sheet |
| Botswana - Mule and ATM information sheet |
| Countries for Money Mules for Africa Scenario |
| Egypt - Mule and ATM information sheet |
| Ethiopia - Mule and ATM information sheet |
| Ghana - Mule and ATM information sheet |
| Kenya - Mule and ATM information sheet |
| Madagascar - Mule and ATM information sheet |
| Malawi - Mule and ATM information sheet |
| Mauritania - Mule and ATM information sheet |
| Mauritius - Offender and ATM information sheet |
| Morocco - Mule and ATM information sheet |
| Mozambique - Mule and ATM information sheet |
| Namibia - Mule and ATM information sheet |
| Nigeria - Mule and ATM information sheet |
| Reunion - Mule and ATM information sheet |
| Senegal - Mule and ATM information sheet |
| South Africa - Mule and ATM information sheet |
| Swaziland - Mule and ATM information sheet |
| Tanzania - Mule and ATM information sheet |
| Tunisia - Mule and ATM information sheet |
| Uganda - Mule and ATM information sheet |
| Zambia - Mule and ATM information sheet |

|  |
| --- |
| **\Evidence files\Money Mule Bank Accounts** |
| 2015-03-31 - Exchange Rates for Mule Bank Accounts |
| Bank Statement Template for victim HSBC |
| HSBC Bank Statement for Algeria Mule |
| HSBC Bank Statement for Angola Mule |
| HSBC Bank Statement for Botswana Mule |
| HSBC Bank Statement for Egypt Mule |
| HSBC Bank Statement for Ethiopia Mule |
| HSBC Bank Statement for Ghana Mule |
| HSBC Bank Statement for Kenya Mule |
| HSBC Bank Statement for Madagascar Mule |
| HSBC Bank Statement for Malawi Mule |
| HSBC Bank Statement for Mauritania Mule |
| HSBC Bank Statement for Mauritius Mule |
| HSBC Bank Statement for Morocco Mule |
| HSBC Bank Statement for Mozambique Mule |
| HSBC Bank Statement for Namibia Mule |
| HSBC Bank Statement for Nigeria Mule |
| HSBC Bank Statement for Reunion Mule |
| HSBC Bank Statement for Senegal Mule |
| HSBC Bank Statement for South Africa Mule |
| HSBC Bank Statement for Swaziland Mule |
| HSBC Bank Statement for Tanzania Mule |
| HSBC Bank Statement for Tunisia Mule |
| HSBC Bank Statement for Uganda Mule |
| HSBC Bank Statement for Zambia Mule |

|  |
| --- |
| **\Evidence files\Steganography** |
| Card data for photo |
| Card stripe information |
| car-original |
| car-original |
| car-original2 |
| car-stego |
| car-stego-new |
| creditcards |
| Setup-OpenStego-0.5.2 |
| stego-instruction |

**Evidence from Suspect Computer**

A virtual machine was created which purports to be an image of the computer of the primary offender Ralph Muller. This device is available on a USB drive. This was created for the 2012 course, not for the 2015 update. It may provide assistance to any trainers that wish to create such a resource in the future. For the 2015 update, the evidence from the suspect computer is provided in the PowerPoint presentation at Session 1.3.2

1. The European Union/Council of Europe Joint Project CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime) is aimed at strengthening the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime. [↑](#footnote-ref-1)
2. All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo [↑](#footnote-ref-2)