|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | **Council of Europe Judicial Training Basic Course DRAFT TIMETABLE** | | | | | | | |
|  | **09:00-09:30** | **09:30-10:00** | **10:00-10:30** | **10:30-11:00** | **11:00-11:30** | **11:30-12:00** | **12:00-12:30** | **12:30-13:00** | **13:00-14:00** | **14:00-14:30** | **14:30-15:00** | **15:00-15:30** | **15:30-16:00** | **16:00-16:30** | **16:30-17:00** |
| **Day 1** | **1.1.1 Course Opening and Introductions** **1 hr** | | **BREAK** | **1.1.2 Introduction to Cybercrime**   **1 hr** | | **1.1.3 Introduction to Financial Investigations 1.5 hrs** | | | **BREAK** | **1.1.4 Introduction to Financial Intelligence Units and the Money Laundering Offence 1.5 hrs** | | | **BREAK** | **1.1.5 Identifying Suspects on the Internet 1 hr** | |
| **Day 2** | **1.2.1 Daily Review 30 min.** | **1.2.2 Electronic Evidence**  **1 hr** | | **BREAK** | **1.2.3**  **Online Criminal Money Flow Typologies** 2 **hrs** | | | | **BREAK** | **1.2.4 Online Criminal Money Flow Typologies**  **1 hr** | | **BREAK** | **1.2.5**  **International Cooperation Methodologies** **1 hr** | | **1.2.6**  **Course Closure**  **30 mins** |

****

**iPROCEEDSf**Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Version 16 May 2017 |

**Training Course for Judges and Prosecutors**

**Basic Course on the Search, Seizure and Confiscation of Online Crime Proceeds**

**Training Manual and Resource Pack**

|  |  |
| --- | --- |
| **Contact:**  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 |

**Table of 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 9

3.4 Course objectives 9

3.5 Target students and trainers group 9

3.5.1 Students 9

3.5.2 Experience Prerequisites 10

3.5.3 Trainers 10

3.5.4 Experience Prerequisites 10

3.6 Resources 10

3.6.1 Course Resources requirements 10

3.6.2 Course Resources customisation 10

3.7 Assessment 10

3.8 Timetable 11

3.9 Course and lesson objectives 12

4 Key Contacts 14

5 Lesson Plans 15

Lesson: 1.1.1 – Course Opening and Introductions 15

Lesson: 1.1.2 – Introduction to Cybercrime 20

Lesson: 1.1.3 – Introduction to Financial Investigations 23

Lesson: 1.1.4 – Introduction to Financial Intelligence Units and the Money Laundering Offence 47

Lesson: 1.1.5 – Identifying Suspects on the Internet 64

Lesson: 1.2.1 – Daily Review 73

Lesson: 1.2.2 – Electronic Evidence 74

Lesson: 1.2.3 – Online Criminal Money Flow Typologies (Part 1) 83

Lesson: 1.2.4 – Online Criminal Money Flow Typologies (Part 2) 94

Lesson: 1.2.5 – International Cooperation Methodologies 99

Lesson: 1.2.6 – Course Closure 110

6 Evaluation 111

7 Assessment 111

8 Appendix 1 Error! Bookmark not defined.

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

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

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

In this context, 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)training materials on cybercrime and electronic evidence have been developed to be used by training institutions.

Considering the success and demonstrated value of the basic and advanced training for judges and prosecutors on cybercrime and electronic evidence, through the European Union and Council of Europe Joint Project iPROCEEDS[[2]](#footnote-2) a further two training modules: a basic and an advanced module on the investigation, search, seizure and confiscation of online crime proceeds were developed. This Training Manual and Resource pack along with the presentations forms part of the basic course.

In general terms, the activities of criminals and criminal organisations are designed to generate profits. According to United Nations estimates, the total amount of criminal proceeds in 2009 was approximately USD2.1 trillion, or 3.6% of global GDP, but only a very small proportion of those funds is ever recovered[[3]](#footnote-3). Targeting proceeds of crime by conducting a financial investigation in parallel with the criminal investigation might also reveal evidence of the money laundering offence. Money laundering allows criminal organisations to benefit from their illegal activities and maintain their operations.

The financial impact of cybercrime and the size of related proceeds are hard to quantify in the absence of reliable data and research, but cases show that the proceeds from cybercrime are laundered through sophisticated schemes involving both traditional and new payment methods[[4]](#footnote-4).

The issues of cybercrime, electronic evidence, crime proceeds and money laundering cut across different institutions and involve, in particular, cybercrime units, financial investigation units, Financial Intelligence Units (FIUs) and prosecution services. However, cybercrime investigations are rarely accompanied by financial investigations and vice versa, investigations of financial or other crimes are rarely accompanied by cybercrime investigations.

Organised crime groups hide and reinvest assets in states other than the one where the crime originating the property was committed. This makes it much more complicated for competent authorities to fight cross-border serious and organised crime. In the same vein, cybercrime and criminal money flows on the Internet do not stop at geographical borders. To address this phenomenon in a comprehensive way, investigative activities should span across the borders and also operate within different jurisdictions. Therefore, effective international cooperation is also crucial for the search, seizure and confiscation of online crime proceeds.

The concept of targeting online crime proceeds presented in this training course brings together the approaches of cybercrime, financial and money laundering investigations with the purpose of increasing efficiency and success of criminal investigations and criminal proceedings from the perspective of both prosecuting a criminal and targeting proceeds of crime. Financial investigation and money laundering prevention and investigation can be related to any profit generating crime, however special attention is devoted to cybercrime (as defined by the Budapest Convention, Articles 2-11) and other types of online crime, where electronic evidence, anonymity and borderless cyberspace are a common challenge.

1. General Overview

## Aim of the Course

This course is designed to introduce judges and prosecutors to the concepts of financial and cybercrime investigations and to study the area of criminal money flows on the Internet, with a particular focus on the search, seizure and confiscation of online proceeds of crime. 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 introduce judges and prosecutors to the unique challenges of investigations of online crime proceeds.

The course will cover the following subjects:

* The basics of financial investigations
* The role and function of a Financial Intelligence Unit (FIU)
* Introduction to cybercrime and cybercrime specific challenges and opportunities
* Introduction to the crime of money laundering
* Understanding online money laundering typologies
* International cooperation methodologies for both cybercrime and financial investigations.

## 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.

Most cybercrime activities are carried out with the intent of generating proceeds of crime. Increased effectiveness when targeting these proceeds of crime will make cybercrime a less attractive form of criminality. The effective operation of all aspects of the judicial system, including effective inter-agency and international cooperation, is necessary to achieve this goal due to the unique characteristics of cybercrime including, for example, the ephemeral nature of digital evidence, the complexities introduced by money laundering on the Internet, the inherently international nature of the Internet and the challenges with collecting evidence from foreign jurisdictions, including from multinational service providers (e.g. Facebook, Google, Microsoft, etc.).

Criminals and criminal groups in general do not limit themselves and their activities to country borders, cybercrime is one type of crime that excludes the need of the offender to travel across borders to commit the crime, thus making the investigation and the prosecution of the perpetrator much harder. This challenge is exacerbated when criminal groups locate proceeds of crime in yet more jurisdictions, further increasing the complexity of the challenges associated with search, seizure and confiscation of online crime proceeds. This emphasises the need for improved international/regional cooperation as well as inter-agency cooperation when dealing with cases of cybercrime.

Increasing use of technology also means that in many cases where a financial investigation is being performed, the predicate offence, the proceeds of crime or the laundering typology involved will coincide with the world of cybercrime and electronic evidence. It is therefore important for those responsible with the investigation, prosecution and adjudication of these matters to have an appreciation of the investigative particularities of cases with both cyber and financial elements.

## The curriculum

This curriculum is a tool to be considered by the training institutions when conducting training on investigation, search, seizure and confiscation of online crime proceeds. The aim of this document is to focus on the establishment and production of harmonised courses or modules that would be used in the carrying out of the initial or in-service training for judges and prosecutors involved in adjudicating or prosecuting such 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, financial and money laundering investigations 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 course has been designed as a mixture of taught lessons and group discussion.

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 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 reflect their national situation. This will ensure a more effective delivery of the course material.

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

This course is designed as a 2-day programme for judges and prosecutors as part of their initial or in-service training 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 investigations. To this end it may be appropriate to utilise the knowledge and skills of those from the law enforcement cybercrime, financial investigation or financial intelligence unit community, as required.

* 1. How will the course be delivered

The course as currently structured should be delivered in classroom setting using classroom based trainer instruction and discussion. As detailed above, in Section 1, trainers will need to adapt the discussion and some content in the programme to reflect the national situation, particularly the relevant provisions in national legislation.

* 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 or during in-service training period that have not taken this course before.

### Experience Prerequisites

This course is designed to be introductory in nature and it is envisioned that participants will have no experience with either financial investigations or cybercrime, or will have experience predominantly with one or the other forms of investigation.

### Trainers

Judicial training centres should employ trainers for this course and should include trainers with experience of conducting cybercrime and financial 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 and financial investigation 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 in classroom layout.
* PC/Laptop running Windows 7, 8 or 10and loaded with MS Office Professional
* Projector and display screen
* Internet access (if available)
* Student notepaper and pens

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

The course discusses the legal matters arising using the framework of relevant international treaties and conventions (e.g. Council of Europe Budapest and Warsaw conventions). It will be necessary for the trainer to identify the relevant provisions in their national legislation for incorporation into the course material. Examples of decisions, forms, templates etc. from national courts relating to cases involving search, seizure and confiscation of crime proceeds will also be required.

* 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

**NOTE: See BasicCourseTimetable.xlsx for an editable version of the timetable.**



* 1. Course and lesson objectives

|  |  |  |
| --- | --- | --- |
| **Session Number** | **Lesson Title** | **Objectives** |
| **1.1.1** | **Course Introduction** | * Identify the trainers and fellow students * 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 * Define course structure and content and explain the aim of combining the cybercrime investigation, parallel financial investigation and money laundering aspects. |
| **1.1.2** | **Introduction to Cybercrime** | * Define the criminal offence of cybercrime as per the Budapest Convention * Define the criminal offence of cybercrime as per national legislation * Explain how cybercrime can be a source of criminal funds * Explain how cybercrime and financial investigations can overlap. |
| **1.1.3** | **Introduction to Financial Investigations** | * Explain the relevance of confiscation of crime proceeds and relation to cybercrime and online investigation * Define what is a financial investigation * Enumerate relevant international legal instruments * Define relevant terms * Understand the four elements of a financial investigation * Describe different confiscation regimes * Explain the relation to money laundering. |
| **1.1.4** | **Introduction to Financial Intelligence Units and the money laundering offence** | * Be able to explain the functions, responsibilities and powers of a financial intelligence unit (FIU) * Understand the types of information that an FIU has access to * Know how FIUs exchange information * Be aware of the relevant international standards * Explain the basic nature of the money laundering offence * Describe the relevance of money laundering to a financial investigation * Provide an example of how FIUs can help with cases involving online crime proceeds. |
| **1.1.5** | **Identifying Suspects on the Internet** | * Know important Internet terminology * Know what is an IP Address * Describe how can you find a suspect IP address * Describe how can you associate a suspect IP address with a real person * List three technical challenges to identification of suspects on the Internet. |
| **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** | **Electronic Evidence** | * Define electronic evidence * Explain how electronic evidence is identified, seized and handled * Explain how electronic evidence is analysed * List the relevant procedural provisions of the Budapest Convention. |
| **1.2.3** | **Online Criminal Money Flows Typologies (Part 1)** | * Explain the criminal money flow typology of the use of money remittance providers * Explain the criminal money flow typology of the use of wire transfers, takeover/opening of accounts * Explain the criminal money flow typology of the use of cash withdrawals * Explain the criminal money flow typology of the use of Internet payment services * Explain the criminal money flow typology of the use of money mules * Explain the criminal money flow typology of the use of international transfers * Explain the criminal money flow typology of the use of virtual currencies * In the case of each typology listed above, list possible sources of evidence * In the case of each typology listed above, list procedural powers in national legislation applicable to the identification of the use of the typology * In the case of each typology listed above, and if applicable, list the procedural powers applicable to the freezing, seizing and confiscation of funds held in an online form. |
| **1.2.4** | **Online Criminal Money Flows Typologies(Part 2)** | * Explain the criminal money flow typology of the use of purchasing through the Internet * Explain the criminal money flow typology of the use of shell companies * Explain the criminal money flow typology of the use of prepaid cards * Explain the criminal money flow typology of the use of online gaming and online trading platforms * In the case of each typology listed above, list possible sources of evidence * In the case of each typology listed above, list procedural powers in national legislation applicable to the identification of the use of the typology * In the case of each typology listed above, and if applicable, list the procedural powers applicable to the freezing, seizing and confiscation of funds held in an online form. |
| **1.2.5** | **International Cooperation Methodologies** | * Explain the relevant of international cooperation in targeting online crime proceeds * Explain the advantages of combining international cooperation avenues in the field of cybercrime and electronic evidence with financial investigation and money laundering * Distinguish international cooperation on exchange of information and on mutual legal assistance * Enumerate relevant international networks and organisations for exchange of information * Describe the nature, purpose and process of mutual legal assistance * Present relevant international legal instruments. * Relevant provisions of the Budapest and Warsaw conventions in order to be able to use them as appropriate. |
| **1.2.6** | **Course Closure** | * Provide appropriate feedback on the course and its effectiveness * Complete the course evaluation forms * Identify the next level of learning needs to further improve 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 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 * Complete relevant administrative tasks * Distribute documentation for the course * Introduce the delegates to the trainers and other delegates * Explain facilities and procedures at the venue including Health and Safety issues * Define the course structure and content and explain the aim of combining the three aspects: cybercrime investigation, parallel financial investigation and money laundering investigation. | | |
| **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” 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. This is a generic presentation that does not take into account national issues that may need to be dealt with when this course is delivered in a particular national training centre. The trainer is responsible for ensuring that the information in this presentation is relevant for the delivery location. | | |
| **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. | | |
| **Slide Notes:** | | |
| **Slide 2** | Health and safety issues are dealt with in this slide. These will differ depending on the location of delivery. It is the trainer’s responsibility to ensure that they have the correct information to impart to delegates. | |
| **Slide 3** | The background of the course is provided for the delegates. The course is developed by the European Union/Council of Europe iPROCEEDS project. | |
| **Slide 4** | The trainer should explain the aims of this session to the delegates. | |
| **Slide 5-8** | The trainer should explain the concept of crime proceeds on the Internet and should focus on these particular aspects:   * Criminal activity, which may or may not be cybercrime, is used by criminals to generate proceeds. * Those proceeds may be laundered, bringing into scope the crime of money laundering. * Those proceeds may not have been laundered, or the laundering offence may not be applicable, but in any event the assets may be searched for, seized, frozen, confiscated.   The focus of this course is on the online money laundering and asset confiscation aspects illustrated in the diagram on slide 5.  Trainer should explain that the relevance of the Internet to these aspects:   * Proceeds may be laundered online, using Internet-based typologies. * Proceeds may be held in various forms on the Internet. * Use of the Internet means that the investigations will almost certainly have an international component.   In general, the activities of criminals and criminal organisations are designed to generate profit[[5]](#footnote-5). Targeting proceeds of crime by conducting financial investigations in parallel to criminal investigations might often also reveal the money laundering offence. Money laundering uses the earnings generated through a multitude of cross-border illegal activities – such as drug trafficking, trafficking in human beings, illicit arms trafficking, corruption and cybercrime – to acquire, convert or transfer property, while hiding the true nature of its origin, in order to use the revenues of these crimes in the legitimate economy. Money laundering allows criminal organisations to benefit from their illegal activities and maintain their operations. Organised crime groups hide and reinvest assets in states other than the one where the crime originating the property was committed. This makes it much more complicated for competent authorities to fight cross-border serious and organised crime.  The Internet-based offences generate proceeds of crime and often the Internet is the place where the laundering process begins. Currently there is general agreement that generating proceeds is now the primary purpose of cybercrime. As highlighted in the Explanatory memorandum to the proposal for an EU directive on counter money laundering by criminal law (22.12.2016), there is a need to address the growing menace of cybercrime and attacks against information systems, in particular attacks linked to organised crime. The financial impact of cybercrime and the size of related proceeds are hard to quantify, in the absence of reliable data and research, but cases show that proceeds from cybercrime are launched through sophisticated schemes, involving both traditional and new payment methods[[6]](#footnote-6). In order to disrupt the financial incentive that drives many cybercrime activities, the proposal qualifies cybercrime, including any of the offences set out in Directive 2013/40/EU[[7]](#footnote-7) as a predicate offence for money laundering.  The concept of targeting online crime proceeds in this training manual brings together the approaches of cybercrime investigation, financial investigation and money laundering investigation with the purpose of increased efficiency and success of both criminal investigations and criminal procedure from the perspectives of both prosecuting a criminal and targeting and confiscating proceeds of crime. Financial investigation and money laundering prevention and investigation can be related to any profit generating crime, however special attention is devoted to cybercrime (as defined by the Budapest Convention in Articles 2-11) and the commission of traditional crimes by means of new technologies, where electronic evidence, anonymity and borderless cyberspace are a common challenge.  Financial investigation is a general method that enables targeting, freezing and confiscation of proceeds of any profit generating crime and is conducted in parallel to a criminal investigation. The aspect of money laundering (prevention and investigation) can be limited to a list of (serious) crimes but many states have an “all crimes” approach, thus money laundering is also relevant when cybercrime is a predicate offence.  The issues of cybercrime, electronic evidence, crime proceeds and money laundering cut across different institutions and involve, in particular, cybercrime units, financial investigation units, Financial Intelligence Units (FIUs) and prosecution services. However, cybercrime investigations are rarely accompanied by financial investigations and vice versa, investigations of financial or other crimes are rarely accompanied by cybercrime investigations. To this end, there is a need for more effective inter-agency cooperation between all these institutions, which is expected to have the strongest impact on the search, seizure and confiscation of online crime proceeds.  As the use of and reliance on information technology becomes ever more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and sophistication, but there has been a time lag in developing effective countermeasures. The evidence derived from electronic devices is volatile, often intangible and probably in another jurisdiction. The identification, collection and preservation of electronic evidence is often vital for a successful criminal investigation. Criminal proceedings increasingly entail cybercrime or electronic evidence found on computer systems or storage devices. Similarly, this argument also applies to the identification, search, seizure and confiscation of online crime proceeds.  Cybercrime and criminal money flows on the Internet do not stop at geographical borders. Therefore, to address these phenomena in a comprehensive way, investigative activities should span across borders and also operate within different jurisdictions. Therefore, effective international cooperation is also crucial for the search, seizure and confiscation of online crime proceeds. Linking the tracing of proceeds of crime and anti-money laundering measures with investigations on cybercrime and computer forensics offers added opportunities. For example, provisional measures to freeze assets could be accompanied by requests for the expedited preservation of electronic evidence. This is one of the reasons that Recommendation 36 of the Financial Action Task Force proposes implementation of the Budapest Contention on Cybercrime and the 2005 Warsaw Convention.  The Warsaw Convention requests parties to adopt legislative measures to facilitate the prevention, investigation and prosecution of money laundering as well as the effective freezing and confiscation of proceeds and instrumentalities of crime and international cooperation.  The Budapest Convention defines cybercrime (Articles 2-11), the investigative measures and international cooperation measures that are applicable not only to cybercrime but also to any type of crime involving electronic evidence.  Better results can be achieved by exploring the possibilities for international cooperation in cross border cases involving cybercrime, other types of computer-enabled crimes and targeting proceeds of such crime by using the various avenues that are provided both by the Budapest and Warsaw conventions.  Time is very important when criminals are hiding behind IP addresses, using optical cables to virtually travel to different countries and leaving their fingerprints in the form of bytes on hard disks, servers, in the cloud and charging for their criminal activity not only by e-banking but also in virtual currency such as bitcoins. The question “where is the money (from)” might lead to the identification of a criminal network. By focussing also on the elements of the money laundering offence when conducting financial investigations in parallel to cybercrime investigations (and computer enabled crime investigation), the powers of FIUs can also be invoked. These include temporary postponement of financial transactions (domestically and abroad), analysis of suspicious transactions, analysis of bank data and also the ability to quickly receive information on bank data from abroad. | |
| **Slide 9** | Following on from the explanation on the previous slide, the trainer should explain why this training is necessary. | |
| **Slide 10** | The trainer should talk through the timetable. | |
| **Slide 11** | The trainer should ask the delegates to pair up, introduce themselves and talk for a few minutes. The delegates should then introduce their partner to the class, and explain the points outlined on this slide. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.1.2 – Introduction to Cybercrime | | **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 * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Aim:** To provide the delegates with information about the substantial criminal offence of cybercrime as defined in the Budapest Convention and their national legislation. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Define the criminal offence of cybercrime as per the Budapest Convention * Define the criminal offence of cybercrime as per their national legislation * Explain how cybercrime can be a source of criminal funds * Explain how cybercrime and financial investigations can overlap. | | |
| **Introduction:**  This session provides information on the criminal offence of cybercrime, for those who have no familiarity with these topics. Note that the trainer will need to be familiar with the substantial and procedural provisions of the Budapest Convention. Additionally, the trainer should familiarise themselves with the explanatory notes to the Budapest Convention and should base their descriptions in this lesson on those explanatory notes.  All information about this session is included in the PowerPoint presentation entitled “Session 1.1.2 – Introduction to Cybercrime” 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. | | |
| **Slide Notes** |  | |
| **Slide 3** | The trainer should ask the students to consider what cybercrime is and ask the students for any examples of cybercrimes they can think of. The responses provided by the students should be noted down on a whiteboard, flipchart etc. for reference later. | |
| **Slide 5, 6** | Trainer should briefly introduce the Budapest Convention, explaining that it includes substantial and procedural provisions, as well as avenues for international cooperation. | |
| **Slide 7** | NOTE: The trainer should familiarise themselves with the explanatory notes to the Budapest Convention and should base their descriptions in this lesson on those explanatory notes.  Trainer should highlight that the offences defines accessing the whole or any part of the computer system without right.  Trainer should highlight the requirement that such access must be intentionally made. | |
| **Slide 14** | The trainer should highlight that Article 9 criminalises possession of child pornography, which is not covered in many legislations. | |
| **Slide 16** | Trainer should explain that most national legislations already criminalise attempt and aiding or abetting of crimes in general in their procedural code. | |
| **Slide 20-28** | Trainer should update these slides to describe the relevant provisions in their national legislation by which the various offences listed above are/are not transposed. | |
| **Slide 29** | The trainer should ask the students to consider which provisions from the Budapest Convention and from their national legislation are applicable in the following scenarios:   1. Ransomware 2. Phishing 3. Hacking a website 4. Running a website for distribution of child pornography 5. Hacking a person’s WiFi and listening to their web browsing activity 6. Conducting a denial of service attack on a website 7. The attempt to misuse stolen payment card data 8. ATM skimming 9. Sharing movies or games on the Internet   The trainer should ask the participants to provide other examples of computer-related crimes and, through guided discussion, help the students to consider how to categorise these crimes under the relevant provisions of the Budapest convention and their national legislation.  The trainer should refer back to the list of offences identified by the students at the beginning of the lesson. | |
| **Slide 30** | Trainer should provide information here on the national cybercrime landscape, indicating common types of cybercrime and information, for example, on number of cases prosecuted under the relevant provisions. | |
| **Slide 31** | Trainer should explain that the following slides are intended to explain how cybercrime offences generate proceeds for criminals. This will be achieved through the use of two examples (banking malware and ransomware. This will be followed with a discussion of some of the peculiarities of cybercrime as a course of crime proceeds to help understand the relevance of the remainder of the course (financial investigations, FIUs). | |
| **Slide 32** | The trainer should talk through the example cybercrimes listed on this slide, indicating in each case how money is made by criminals through the crime. | |
| **Slide 33** | Trainer should talk through the specific example of the banking malware and how it works at a high level. | |
| **Slide 34** | Trainer should talk through the specific example of ransomware and how it works at a high level. | |
| **Slide 35** | Trainer should highlight the point that the amounts of money generated by individual crimes are usually small, but when these amounts are aggregated over a large number of victims the total criminal proceeds are significant. | |
| **Slide 36** | Trainer should highlight the fact that mules are a key component of many cybercrime operations. This will be discussed later in detail (on the second day) but trainer should highlight specifically that mules often have no idea about the cybercrime components of the criminal enterprise. | |
| **Slide 38-39** | Trainer should explain that targeting online crime proceeds can be considered from three perspectives: financial investigation, cybercrime investigation and money laundering prevention and investigation. The particularities of the three aspects are relevant for investigative phase, the judicial phase and the international cooperation. | |
| **Slide 40 and 41** | The four elements, described in the introduction to financial investigations (Lesson 1.1.3), that are relevant for financial investigations, can be exercised also in cybercrime.  There are some specifics:   * Who is the perpetrator and evidence of the crime: IP ID, - access to data on user, traffic and content, cooperation with ISP, court order (traffic and content data) * What are the proceeds of crime: often the e-money, bitcoins and internet banking payments; accounts abroad, multiple transactions, often money laundering typologies; virtual currencies. * What can be confiscated/the property of suspect: There is also a question of jurisdiction, victims and perpetrator are often not in the same country. But the confiscation of proceeds of cybercrime, through FI or money laundering approach should be considered. Focus and target at least on direct proceeds of crime (extortions paid or fraudulent transactions) and the freezing of value in identified bank accounts used for criminal offence (cyber extortion, cyber fraud). * If the perpetrator is in your country explore legal ways with other countries to be more efficient (parallel criminal investigations in two countries (several criminals, several victims). * Conduct parallel financial investigation to detect the proceeds (bank accounts and money flow) and the existing property of perpetrator. * Freezing order: acting fast is crucial in case of e-banking and internet world. Look for money laundering offence and use FIU powers and international links. Court order and MLA shall follow quickly. Use of Interpol channel for MLA, Warsaw convention and additional possibilities of Budapest convention, bilateral agreements and reciprocity approach.   Confiscation: question of MLA and asset-sharing. Importance of timely freezing!  Trainer should explain that the issues of electronic evidence, online typologies and international cooperation for investigation/search/seizure/confiscation in cybercrime matters will constitute the bulk of the remainder of the course. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.1.3 – Introduction to Financial Investigations | | **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 financial investigations. | | |
| **Objectives:**   * Explain the relevance of confiscation of crime proceeds and relation to cyber (and online) crime investigation * Define what is a financial investigation * Enumerate relevant international legal instruments * Define relevant terms * Understand the four elements of a financial investigation * Describe different confiscation regimes * Explain the relation to money laundering. | | |
| **Introduction**  This session provides basic information on financial investigations, for those who have no familiarity with financial investigations.  All information about this session is included in the PowerPoint presentation entitled “Session 1.1.3 – Financial Investigations” 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 | | |
| **Slide Notes** |  | |
| **Slide 5** | One of the main motives of serious and organised crime, including cybercrime, is financial gain. Among the most effective means of combating organised crime is detection, freezing and confiscation of instrumentalities and proceeds of crime.  The confiscation of proceeds of crime has numerous effects:   * Preventative, as economic profit is the rationale of most criminal offences; * It prevents the infiltration of illegal profits and corruption into the legal economy; * It removes the instrument to commit future crimes; * It helps to target the top management of a criminal organisation; * It upholds the rule of law and the principle that nobody should benefit from crime.   The confiscation system and procedure can be divided into three phases:   1. Investigative phase - financial investigation, where proceeds of crime are identified and located and evidences on its/their owner(s) (and information on his/their property) are collected. The result of the financial investigation can be a temporary measure (freezing) of property to secure later confiscation ordered by the court. 2. Judicial phase, where the defendant is convicted (or acquitted) and the decision on confiscation is final. 3. Disposal phase, where the property is actually confiscated and disposed by the State in line with the law, while taking into account international asset sharing. | |
| **Slide 6** | Financial investigation can have several meanings, for example investigation of financial crime or investigation for taxation purposes. International legal instruments do not provide for definition of financial investigation, but in the framework of freezing and confiscation of proceeds of crime the descriptive definition provided by the Financial Action Task Force (FATF) can be used as an example.    It should also be noted that the term “financial investigation” might include both investigation for targeting proceeds of crime in the framework of criminal procedure as well as in a (separate) civil (in rem) procedure. It should also be noted that financial investigation can (but does not necessarily) coincide with a **money laundering** investigation.  Financial investigations are an investigative method that should be conducted in parallel to a criminal investigation of a profitable crime. Financial investigation can be, according to national legislation, carried out also in the judicial phase with the main (but not exclusive) purpose of tracing and freezing proceeds of crime with a view of their final confiscation.  Financial investigation has been defined by the FATF[[8]](#footnote-8) as an enquiry into the financial affairs related to a criminal activity, with a view to:   * Identifying the extent of criminal networks or the scale of criminality; * Identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and * Developing evidence that can be used in criminal proceedings.   A ‘parallel financial investigation’ refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorized to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.  As the criminal profits tend to be legalised and at least partly re-used in legal economy, financial investigation might be related or/and lead to a **money laundering** investigation. The financial investigation can lead to a suspicion of the criminal offence of **money laundering.** Alternatively, when a Financial Intelligence Unit (FIU) is analysing suspicious transactions, or investigating the criminal offence of **money laundering**, proceeds from (predicate) crime could become the subject of confiscation (as an object of a **money laundering** crime).  **The trainer should ask the students to discuss what is their national definition of financial investigation? The trainer should, after discussion, provide the national definition of financial investigation if it is not known to the delegates.** | |
| **Slide 7-8** | “No one should benefit from crime and keep the proceeds from crime.”  This principle has also been developed at the international level. It provides for (i) a legal obligation of Parties to establish measures to trace, freeze and confiscate proceeds from crime and (ii) a legal framework for international cooperation, including mutual legal assistance.  International instruments provide for:   * a legal obligation of Parties to establish measures to trace, freeze and confiscate proceeds from crime and * a legal framework for international cooperation, including mutual legal assistance.   The United Nations has also developed legal instruments dealing with the topic that provide for a (global) framework. The trainer should provide some examples of them, the particularly relevant conventions being the conventions against drugs (United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 19.12.1988), transnational organised crime (United Nations Convention Against Transnational Organised Crime, New York, 15.11.2000) and corruption (United Nations Convention Against Corruption, New York, 31.10.2003).  Some international conventions also provide for monitoring mechanisms, which further develop the standards, such as the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), the Group of States Against Corruption (GRECO) or FATF.  However the rules on financial investigation and confiscation of proceeds of crime depend on national legal provisions and jurisprudence, its placement into the criminal (or other) procedure, on powers and relations between the relevant national institutions. For the practical application of standards and elements of financial investigation the knowledge of national law is essential.  Search (tracing), seizure (freezing) and confiscation of the proceeds from crime is a central part of the **2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism**[[9]](#footnote-9)(hereinafter: Warsaw Convention), which succeeded the 1990 Convention on Laundering, Search, Seizure And Confiscation of the Proceeds From Crime[[10]](#footnote-10).  The trainer should clarify that cooperation with parties to Strasbourg Convention is regulated in Article 49, paragraph 6 of Warsaw Convention.  Council of Europe Criminal Law Convention on Corruption (Strasbourg, 1999, ETS 173) also refers to the confiscation of instrumentalities and proceeds of corruption criminal offences. | |
| **Slide 9** | To understand the instruments it is important to explain the meaning of terms. As mentioned, there is no legal definition of financial investigation, but Article 2 of the Directive 2014/42/EU and Article 1 of the Warsaw Convention provide for the following definitions:   * ‘proceeds’ means any economic advantage derived directly or indirectly from a criminal offence; it may consist of any form of property *and includes any subsequent reinvestment or transformation of direct proceeds and any valuable benefits* (last part of the sentence is not included in the Warsaw Convention); * ‘property’ means property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title or interest in such property; * ‘instrumentalities’ means any property used or intended to be used, in any manner, wholly or in part, to commit a criminal offence or criminal offences; * ‘freezing or seizure’ means the temporary prohibition of the transfer, destruction, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority (Directive 2014/42/EU refers only to the term freezing in this context); * ‘confiscation’ means a final deprivation of property ordered by a court in relation to a criminal offence (the Warsaw Convention defines it as a penalty or a measure).   **The trainer should define relevant national legal provisions and compare them with these definitions. The trainer should, in particular, highlight any differences between the relevant national legal provisions and these definitions.** | |
| **Slide 11** | Trainer should explain that financial investigation can be best defined by defining the elements of a financial investigation and identifying relevant international and national legal provisions to be applied in practice.  Broadly, a financial investigation consists of four elements:   1. Detecting the criminal offence and the perpetrator (parallel to criminal investigation) 2. Establishing the proceeds of crime 3. Establishing property that can be confiscated 4. Freezing order - temporary measures for securing the confiscation. | |
| **Slide 12** | **Financial Investigation Element 1: Relationship between criminal investigation and (parallel) financial investigation.**  **Discussion: Trainer should ask students when to start the financial investigation? Also trainer should ask who starts/conducts the financial investigation?**  When investigating a criminal offence (organised, economic or classic crime, including cybercrime) and gathering evidence on the elements of the criminal offence, the perpetrator and co-perpetrators, it is necessary to carry out a parallel financial investigation in cases when the criminal offence results in property benefit. Most crime is done for financial gain, so a financial investigation can also unearth evidence that could help to secure a conviction.  With regard to the fact that the purpose of a financial investigation is to enable the confiscation of proceeds, it has to be started at an early date enough to prevent eventual perpetrator’s disposal of the property. The right time would therefore be after detecting the suspect(s) and before carrying out measures, which inform the perpetrator about an investigation against him (e.g. house search). Financial investigation and analysis of transactions may extend the circle of suspects, and in gathering evidence it is also necessary to consider the aims of the financial investigation (e.g. in wiretapping, seizure of documents, etc.).  The relation to the (predicate) criminal offence is relevant also in the case of non-conviction based (civil) confiscation and in case of money laundering investigation.  More detailed instructions on the conditions concerning the introduction of financial investigation can be issued by the police (or the prosecutor’s office).  In cases of banking malware and ransomware, as forms of cybercrime, defined by the Budapest Convention criminal proceeds are the main motive. More details on the modus operandi are found in the lesson “Introduction to Cybercrime”. Conducting parallel financial investigations and paying attention to the possible money laundering of the proceeds from such predicate offences (such as use of money mules, etc.) could benefit the main aims of the criminal (cybercrime) investigation – to identify criminals and to gather evidence, and could also benefit the financial investigation – to trace, freeze and confiscate proceeds of crime, and also to recover victims of a crime.  It should be highlighted at this point also that the FIU in its preventive capacity might be able to contribute to the initiation of a criminal investigation. Based on analysis of suspicious transaction reports (STRs) and Cash transaction reports (CTRs) the FIU may identify suspicion of money laundering, as well as investigative leads to a predicate offence.  The trainer should highlight the role of the FIU as a source of financial intelligence. As mentioned above, analysis of suspicious transaction reports (STR) and Cash Transaction Reports (CTR) may identify new investigative leads. FIUs may also be used to make informal enquiries with other FIUs. If you suspect the defendant has a bank account in another country then your domestic FIU can make FIU-to-FIU enquiries to establish if any financial footprint exists in the foreign jurisdiction. Knowing the nature of this, and its relevance and applicability, will allow a prosecutor to make a more focused MLA request to obtain the financial data as evidence.  FIUs should also have a good understanding of the regulated sectors in their jurisdiction. Consider asking the FIU to make informal enquiries of the regulated entities to establish if any financial leads on the defendant are known.  **Identify relevant national legal (material and procedural) provisions** obliging responsible authorities to conduct financial investigation – to apply measures to identify, trace, freeze or seize rapidly property which is liable to confiscation in order in particular to facilitate the enforcement of a later confiscation - see the Warsaw Convention Article 4 (Investigative and provisional measures).  **Identify who is responsible for initiating, leading and performing financial investigation.**  Is there a specialised unit in the criminal police responsible exclusively for FI, so the criminal investigators would invite financial investigators to work together?  Are there specialised investigators/prosecutors for financial investigation that can be consulted or engaged in (parallel to) the criminal investigation?  **Warsaw Convention Article 4 (Investigative and provisional measures):** measures to identify, trace, freeze or seize rapidly property which is liable to confiscation in order in particular to facilitate the enforcement of a later confiscation. | |
| **Slide 13** | **Financial Investigation Element 2: Establishing the proceeds of crime.**  **The trainer should recall the definition of ‘proceeds’**: it means any economic advantage derived directly or indirectly from a criminal offence; it may consist of any form of property *and includes any subsequent reinvestment or transformation of direct proceeds and any valuable benefits.*  Proceeds can be an **element of a criminal offence** (especially in crimes against the property or in economic crimes, including computer related fraud). Moreover, direct proceeds constitute evidence of the criminal offence. By detecting proceeds resulting from a criminal offence (e.g. money (or virtual currencies) as payment for online purchase of drugs (e.g. on the Darknet), child pornography, stolen artistic painting or benefit from online financial fraud) and investigating it, co-perpetrators or even organisers of the criminal offence can be detected, as well as third persons from whom proceeds can be confiscated.  Classically, proceeds resulting from a concrete criminal offence under investigation or for which the perpetrator has been convicted are the only property that can practically be confiscated. The connection between the specific criminal offence and the amount of (concealed) proceeds is relaxed to a certain extent in the case of the criminal offence of **money laundering** (when first, the amount of a suspicious transaction is identified). On the other hand, there are legal systems where extended confiscation is applied and reversed burden of proof regarding the origin of property. In addition to confiscating proceeds resulting from the concrete (proved) criminal offence, such systems enable the confiscation of additional property, which under specific conditions is assumed to result from a criminal offence.  Both the direct proceeds and the **indirect proceeds** gained by a criminal offence or because of it (e.g. the perpetrator sells a stolen painting, for the money he buys securities, whose value on the stock market increases) are confiscated.  As a rule, **gross proceeds** are counted, without subtracting the costs the perpetrators has had in order to commit the criminal offence (e.g. remaking a vehicle for illegal transport across the state border).  The establishment of proceeds from a concrete criminal offence represents an important basis both for the implementation of temporary measures and for the final confiscation ordered by the court. Some penal procedural laws enable the court to decide on the amount of confiscated proceeds also **at its own discretion** when the amount cannot be accurately established. However, such a decision must be explained, proportionate and based on the findings and assessment of the financial investigation.  When the direct proceeds cannot be confiscated (e.g. a stolen vehicle), the (legal) property corresponding to such proceeds can be confiscated (value based confiscation system). Freezing is therefore possible on all (including legal) property of the defendant. | |
| **Slide 14** | The ways to **establish the amount and type** of illegal proceeds are various. Sometimes, this is clear from the complaint by the injured person (e.g. theft, fraud (including online fraud), robbery). In such cases, an estimate of the damage can be helpful which, however, does not necessarily equal the illegal proceeds.  In organised crime, the amount and type of proceeds are also established through covert investigation measures, by wiretapping, covert surveillance, undercover operations. For example, in gathering evidence on drug trafficking, it is established how many drugs have been sold, at what price and to whom, to which bank accounts etc. Based on such data, the assessment of the amount of proceeds is prepared. In economic criminal offences, the damage or illegal proceeds are established by the examination of business documents, also in collaboration with the tax service.  In establishing the proceeds, data on the financial transactions carried out by the suspect and other persons are also relevant. As a rule, access to bank data is only possible with a court order and is conditional upon a certain standard of evidence. Through the analysis of payments and money orders, the perpetrator’s financial flow and other related persons are established. In analysing financial flows, it is often necessary to obtain data from abroad. When current data on transactions on a specific bank account are relevant for the investigation, a monitoring order is an important measure, which also enables to immediately prevent a money order from being effected to another account, notably one abroad. In such cases, it is especially important to have good and fast co-operation with the court that issues such orders and the financial institution that implements them.  In case of money laundering the powers of FIU should be considered for the access to bank data, for their analysis, for access to bank data abroad and possibility of administrative freezing. Depending on the particularities of each jurisdiction, the role of the FIU might not be limited to money laundering.  **Virtual currencies**  Virtual currencies, in addition to e-banking are often used as a means of payment for online crime[[11]](#footnote-11), such as purchase of drugs of weapons online, or for receiving payments from extortion victims, or to transform/hide money deriving from crime.  Virtual currencies[[12]](#footnote-12) means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural and legal persons as a means of payment and can be transferred, stored or traded electronically.  Virtual currencies such as bitcoin are not legally considered currency, with some exceptions[[13]](#footnote-13), as they are not issued by licensed bodies (central banks) nor regulated as part of the financial system. The bitcoin wallet is created online and can be saved on a personal computer. Transfers from one wallet to another are done online. Value can be converted to fiat money either online or at specific exchange machines (cash machines). This means that the identification of the holder of bitcoin and the tracing of bitcoin transactions are challenging tasks.  It is important to note that a bitcoin has a market value, and can be considered as property. It should also be possible (with a wallet key) to seize it – transfer it to another wallet and to keep it or exchange it.  More information on virtual currencies is presented in a later session.  **Trainer should ask the students what are the national legal provisions to use special investigative techniques, and to access to bank data (on holder, transactions and monitoring)? See the Convention Article 7.**  **Warsaw Convention Article 7 (Investigative powers and techniques) requires Parties to establish:**   1. measures to empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized Bank secrecy should not prevent it. 2. measures to:  * determine whether a natural or legal person is a **holder** or beneficial owner of one or more accounts in bank and obtain all of the details of the identified accounts; * obtain the particulars of specified bank accounts and of **banking operations** which have been carried out during a specified period through one or more specified accounts, including the particulars of any sending or recipient account; * **monitor**, during a specified period, the banking operations that are being carried out through one or more identified accounts; and, * ensure that banks do not disclose to the bank customer concerned or to other third persons that information has been sought or obtained or that an investigation is being carried out. * Parties shall consider extending this provision to accounts held in non-bank financial institutions.  1. measures to enable it to use **special investigative techniques** facilitating the identification and tracing of proceeds and the gathering of evidence related thereto, such as observation, interception of telecommunications, access to computer systems and order to produce specific documents. | |
| **Slide 15** | **Financial Investigations Element 3: Establishing property that can be confiscated**  Depending on Confiscation regimes, financial investigations can focus on direct/indirect proceeds, property of corresponding value, extended confiscation or even civil (in rem) confiscation.  Criminal offenders usually hide or conceal direct proceeds from crime, as they constitute evidence. In addition to that, they also conceal their property. Namely, when direct proceeds from a criminal offence cannot be confiscated (found), confiscation of (legal) property corresponding to the value of illegal proceeds is possible. An important part of financial investigation is therefore to establish the property owned or controlled by the offender or the persons from whom property can be confiscated.  **Money**  Data on cash money can be obtained through information, interviews, a house search (hidden places, safes, key to a bank safe, etc.). In order to obtain data on a bank account, a court order is usually necessary. Access to data as to which bank accounts the suspect has is also relevant.  Data on bank account holders can be found in the central records of the central bank or within FIU records, otherwise it is necessary to verify data with all the banks and financial institutions[[14]](#footnote-14). Data on the account can also be obtained from income tax or tax returns, profit and loss statements, bank cards or bank statements of account, which can be found during a house search.  Frequent money orders from the bank account to another account (at a foreign bank) may also give rise to suspicion. In analysing bank data, attention also has to be placed on different **money laundering** techniques. But, although money is the type of property that is most easy to be temporarily secured and stored, other types of the suspect’s property also need to be established.  **Securities**  Central records of the holders of securities are normally kept by the Clearing and Depositary Company. The conditions to access such data depend on the national legislation.  Data on ownership of companies that do not list on the stock exchange are evident from the legal entities register (the court), the tax return or the profit and loss statement. The type of registration, data and records are governed by the legislation on companies and tax legislation.  **Movable property**  Records on **vehicles** are normally under the competence of the responsible Ministry. Attention should also be placed on vehicles that the suspect uses although they are not formally his property. The circumstances of such use should be investigated (leasing, formal ownership by a friend, a partner, etc.). As regards vessels and aircrafts, central records of their owners are normally kept. Data on ownership of more valuable movable property (e.g. **artistic** paintings) can be obtained from the insurance companies that ensure such property.  In addition, possession and ownership of movable property can be established during a house search.  **Real estate**  The source of information is the **land register**. If the land register does not consist of up to date centrally computer kept records, obtaining data can be more difficult. If the land register is kept by local courts, data should be verified with those courts. Data on ownership can normally also be obtained from the tax service (real estate trade tax, real estate tax).  Virtual currency should also be considered, especially if relevant for the crime in question (see previous section).  **Property abroad**  The offenders may also hide (have) their property abroad. See the Mutual legal assistance part.  Data on a person’s **income and property** can be obtained from the income tax return (natural persons) or the tax return or the profit and loss statement (companies). For this reason, a good co-operation with the **tax service** (and proper legal basis) is important in order to access their records.  Financial investigation can also reveal **disproportion between** the suspect’s legal (reported) property and his actual property. This is relevant in legal systems where extended confiscation of proceeds is possible and where the offender has to rebut the Prosecutor’s assertion of illegal origin of the property, otherwise the property may be confiscated (the reverse burden of proof).  **Financial investigation should focus on relevant third and legal persons.**  If the **perpetrator** transfers the proceeds to another person who is aware that they result from a criminal offence, that person can be responsible as the concealer or for the money laundering and the proceeds are confiscated. Moreover, it is also possible to confiscate **property from third persons** who obtained a property benefit (an object) for a non-market value and should or could have known that it might originate from a criminal offence and from perpetrator’s close relatives. Proceeds have to be subject to confiscation even in case when they are transferred to a legal entity.  In order to implement financial investigation, **interdisciplinary knowledge** and knowledge of a wide spectrum of legislation (civil, bank, tax, securities, and companies) is necessary. The existing records and access to data depend on the national legislation, and the above ways to establish property are listed only as an example. Financial investigation is facilitated and made quicker if the necessary records are in place, if they are kept up to date and if quick access to data is provided, which again implies a good co-operation with different institutions.  Being familiar with the rules regarding access to data and contact persons in institutions is therefore of great importance for financial investigators.  (Tactical) decision is to be taken whether to focus on tracing the proceeds from concrete criminal offence at the initial phase (parallel criminal and FI) and the extended scope will follow after the evidence for criminal offence is gathered (and secured) and person is arrested/accused. Especially if there is a danger to reveal the conduct of covert criminal investigation by contacting different institutions to identify the property of a suspect.  **Warsaw Convention Article 5 (Freezing, seizure and confiscation)** require that measures to freeze, seize and confiscate also encompass:   * the property into which the proceeds have been transformed or converted; * property acquired from legitimate sources, if proceeds have been intermingled, in whole or in part, with such property, up to the assessed value of the intermingled proceeds; * income or other benefits derived from proceeds, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, up to the assessed value of the intermingled proceeds, in the same manner and to the same extent as proceeds.   **Directive 2014/42/EU Article 6 (Confiscation from a third party)**   1. Member States shall take the necessary measures to enable the confiscation of proceeds, or other property the value of which corresponds to proceeds, which, directly or indirectly, were transferred by a suspected or accused person **to third parties**, or which were acquired by third parties from a suspected or accused person, at least if those third **parties knew or ought to have known that the purpose of the transfer** or acquisition was to avoid confiscation, on the basis of concrete facts and circumstances, including that the transfer or acquisition was carried out free of charge or in exchange for an amount significantly lower than the **market value**. 2. Previous paragraph shall not prejudice the rights of bona fide third parties.   **Trainer should describe for the students the national legal provisions on property that can be confiscated including from third person – see the Warsaw Convention Article 5 and Directive 2014/42/EU Article 6?**  **Trainer should describe for the students the national legal provisions for the access to bank data, stocks, land register, movable property, tax reports and for cooperation with relevant institutions, such as tax office?** | |
| **Slide 16 and 17** | **Financial Investigation Element 4: Freezing order – temporary measures for securing confiscation**  **Trainer should recall for the students the definition of ‘freezing or seizure’**: meaning the temporary prohibition of the transfer, destruction, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority (Directive 2014/42/EU refers only to the term freezing in this context).  The purpose of temporary measures for securing property is to prevent disposal, transfer or hiding of proceeds or the offender’s property and to enable final confiscation. The temporary measure for securing property is an essential result of the financial investigation, if legal conditions exist.  The measures are defined in the criminal procedural legislation, which in some countries also refer to civil executive legislation (temporary orders).  **Can the police seize property (other than direct proceeds) during house search to secure value based confiscation?**  As regards seizing objects, police powers normally cover objects used to commit a criminal offence (instrumentalities), objects that resulted from a criminal offence, and evidence. The police can thus only seize the direct proceeds that have resulted from the criminal offence and the evidence (stolen vehicle, banknotes resulting from a bank robbery, etc.).  **Would a consequent court freezing order be required to allow for legal remedies?**  **Freezing (temporary securing) order**  Temporary securing order is issued by the (investigative) judge upon the proposal by the prosecutor’s office (based on the report on financial investigation from the police). The proposal to issue a temporary securing order is given upon the conclusion of a financial (and classic) police investigation, together (or not) with the crime report, and before the institution of court proceedings, when the offender is informed about the evidence burdening him. **This is why it is important for the legislation to enable the issue of an order also during the pre-trial procedure.**  A proposal can also be given before the conclusion of a police investigation, if there is danger of disposal (e.g. the person wishes to send a money order abroad, intends to sell his property, etc.), although care should be taken that the investigation of the criminal offence and gathering of the necessary evidence are not jeopardised by this measure. Careful weighing is especially required in lengthy and more demanding investigations of organised crime.  The conditions, procedure and contents of a freezing order are defined by the national legislation. The proposal for temporary securing of property, which results from financial investigation, has to comprise all the necessary elements for the issue of an order.  Normally, the conditions for the issue of an order are as follows:   * probability (or a standard of evidence higher than grounds for suspicion) of the existence of a criminal offence and the resulting proceeds (the amount), * danger of the offender’s disposal of hiding or destroying the proceeds or making seizure impossible in some other way.   **The proposal** has to include the results of the financial investigation:   * findings and evidence in relation to the criminal offence and the perpetrator (this is normally part of the crime report), * findings on the type and amount of the illegal proceeds, * findings on the property that can be seized and proposal as to which property is to be secured and the persons it belongs to, indication as to whether any property has already been seized, * grounds for the legal conditions for the issue of an order (standard of evidence, danger of disposal)[[15]](#footnote-15).   In some countries the criminal legislation regarding the conditions of ordering temporary measures instructs to apply the rules of the executive procedure.  **Trainer should describe for the students the relevant national legal provisions for freezing order and its conditions? See also Directive 2014/42/EU Article 7 and 8 and Warsaw Convention Article 5 and 8.**  **Trainer should ask the students to discuss when to request a freezing order and to consider the consequence for criminal investigation.**  **Trainer should also explain the possibility of temporary suspension of a transaction by FIU in case of money laundering**. Take into account the speed and time limits of FIU freezing. – This will be discussed later in the lesson on FIUs.  The trainer should provide a template for a proposal for freezing order (prosecutor) and a template of a freezing order (court order).  Directive 2014/42/EU Article 7 (Freezing)   1. Member States shall take the necessary measures to enable the freezing of property with a view to possible subsequent confiscation. Those measures, which shall be ordered by a competent authority, shall include urgent action to be taken when necessary in order to preserve property. 2. Property in the possession of a third party, as referred to under Article 6, can be subject to freezing measures for the purposes of possible subsequent confiscation.   **Directive 2014/42/EU Article 8 (Safeguards)**   1. Member States shall take the necessary measures to ensure that the persons affected by the measures provided for under this Directive have the right to an **effective remedy** and a fair trial in order to uphold their rights. 2. Member States shall take the necessary measures to ensure that the freezing order **is communicated** to the affected person as soon as possible after its execution. Such communication shall indicate, at least briefly, the reason or reasons for the order concerned. When it is necessary to avoid jeopardising a criminal investigation, the competent authorities may postpone communicating the freezing order to the affected person. 3. The freezing order shall remain in force only for as long as it is necessary to preserve the property with a view to possible subsequent confiscation. 4. Member States shall provide for the effective possibility for the person whose property is affected to **challenge the freezing order before a court**, in accordance with procedures provided for in national law. Such procedures may provide that when the initial freezing order has been taken by a competent authority other than a judicial authority, such order shall first be submitted for validation or review to a judicial authority before it can be challenged before a court. 5. Frozen property which is not subsequently confiscated shall be **returned immediately**. The conditions or procedural rules under which such property is returned shall be determined by national law. 6. Member States shall take the necessary measures to ensure that **reasons are given for any confiscation order** and that the order is **communicated** to the person affected. Member States shall provide for the effective possibility for a person in respect of whom confiscation is ordered to challenge the order **before a court**. 7. Without prejudice to Directive 2012/13/EU and Directive 2013/48/EU, persons whose property is affected by a confiscation order shall have the right of access to a lawyer throughout the confiscation proceedings relating to the determination of the proceeds and instrumentalities in order to uphold their rights. The persons concerned shall be informed of that right. 8. In proceedings referred to in Article 5, the affected person shall have an effective possibility to challenge the circumstances of the case, including specific facts and available evidence on the basis of which the property concerned is considered to be property that is derived from criminal conduct. 9. Third parties shall be entitled to claim title of ownership or other property rights, including in the cases referred to in Article 6. 10. Where, as a result of a criminal offence, victims have claims against the person who is subject to a confiscation measure provided for under this Directive, Member States shall take the necessary measures to ensure that the confiscation measure does not prevent those victims from seeking compensation for their claims.   **Warsaw Convention Article 8 (Legal remedies):** measures to ensure that interested parties affected by such measures shall have effective legal remedies in order to preserve their rights. | |
| **Slide 18** | **Trainer should ask the students to discuss what issues will influence the nature and scope of the application for the freezing order.**  Through guided discussion, the trainer should get the students to consider:   * the relevant national provisions for the freezing order and its conditions (see also Directive 2014/42/EU Article 7 and 8 and Warsaw Convention Article 5 and 8) * When to propose/issue the freezing order – consider the consequence for the criminal investigation. * What property to freeze * Consider temporary suspension of transaction by FIU in case of money laundering. Take into account the speed and time limits of FIU suspension.   At the end of the discussion, and if possible, the trainer should provide the students with an example of a court freezing order prepared under the national legislation. | |
| **Slide 20** | **Financial Investigation Element 4: Confiscation of proceeds of crime**  **Trainer should recall for the students the definition of ‘confiscation’**: it means a final deprivation of property ordered by a court in relation to a criminal offence (the Warsaw Convention defines it as a penalty or a measure).  Proceeds are confiscated with a judgment of conviction. The court decides on the confiscated amount and the type of confiscation. In case of non-conviction based (civil) confiscation judgment of conviction is not necessary for confiscation of proceeds but there is a special civil procedure in place (for example in Ireland, UK, Slovenia etc.).  In cases where the proceeds constitute an element of the criminal offence, the court must decide on their confiscation. The prosecutor proposes confiscation during the trial and if the court does not take a decision, this constitutes grounds for appeal. If the legislation allows it, the confiscation is also possible without a judgment of conviction, upon the conclusion of the criminal procedure (e.g. due to the defendant’s death or the criminal offence becoming statute barred).  In any case, the confiscation of proceeds is possible if the property has been temporarily secured. Otherwise there have been numerous cases when at the end of the criminal procedure the perpetrator had no property left, as he had disposed of it or hidden it.  **Trainer should explain the national legal provisions on confiscation – see the Warsaw Convention Article 3 and Directive 2014/42/EU Article 4, 6 and 9?**  **Trainer should also discuss the issue of confiscation in cases where proceedings are stopped (e.g. death of defendant).**  **Directive 2014/42/EU Article 4 (Confiscation)**   1. Member States shall take the necessary measures to enable the confiscation, either in whole or in part, of instrumentalities and proceeds or property the value of which corresponds to such instrumentalities or proceeds, subject to a final conviction for a criminal offence, which may also result from proceedings in absentia. 2. Where confiscation on the basis of paragraph 1 is not possible, at least where such impossibility is the result of illness or absconding of the suspected or accused person, Member States shall take the necessary measures to enable the confiscation of instrumentalities and proceeds in cases where criminal proceedings have been initiated regarding a criminal offence which is liable to give rise, directly or indirectly, to economic benefit, and such proceedings could have led to a criminal conviction if the suspected or accused person had been able to stand trial.   Directive 2014/42/EU Article 6 (Confiscation from a third party): See part 2.3.  Directive Article 9 (Effective confiscation and execution)  Member States shall take the necessary measures to enable the detection and tracing of property to be frozen and confiscated even after a final conviction for a criminal offence or following proceedings in application of Article 4(2) and to ensure the effective execution of a confiscation order, if such an order has already been issued.  **Warsaw Convention Article 3 (Confiscation measures)** necessary measures to **confiscate instrumentalities and proceeds or property the value** of which corresponds to such proceeds and laundered property.   1. (ML reservation – see 9/4 + evaded tax ) 2. Parties **may** provide for mandatory confiscation in respect of offences which are subject to the confiscation regime. Parties may in particular include in this provision the offences of money laundering, drug trafficking, trafficking in human beings and any other serious offence. | |
| **Slide 21** | When it is possible to enforce a property claim due to the damages suffered by the criminal offence under the criminal procedure, such a claim has precedence over the confiscation of proceeds. The injured party can file the property claim at the same time as he files the complaint to the police concerning the criminal offence. The court has to decide on such a claim, except in cases when such decision-making would disproportionately prolong the criminal procedure, in which case the injured party is instructed to start a civil action. If the court decides on the claim, the confiscated proceeds are used to pay the damages first and the remainder of the illegal proceeds becomes part of the budget.  What are the relevant national provisions?  Directive 2014/42/EU Article 8 (Safeguards)  10.   Where, as a result of a criminal offence, victims have claims against the person who is subject to a confiscation measure provided for under this Directive, Member States shall take the necessary measures to ensure that the confiscation measure does not prevent those victims from seeking compensation for their claims. | |
| **Slide 22** | Experience in practice shows that proving the criminal origin of offender's property is in many cases very difficult or impossible.  The introduction of reversal of burden of proof of the origin of the property (not of guilt!) has been promoted by international legal instruments including the Warsaw Convention and Directive 2014/42/EU. Some countries are using such solutions in practice. Also the jurisprudence of European Court for Human Rights confirms that such approach under specific conditions is compliant with human rights standards of the European Convention on Human Rights: the right to a fair trial, the presumption of innocence and the protection of property Article 1 of the Protocol No. 1 to the European Convention (See Case *Minelli vs. Switzerland*, 1983, Case *Salabiaku vs. France*, 1988, Case *Murray vs. UK*, 1996, Case *Saunders vs. UK*, 1996, Case *Welch vs. UK*, 1995, Case *Phillips vs. UK*, 2001 etc.).  The recent **Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union** replaced the relevant provisions of Article 3 of **Framework Decision 2005/212/JHA** on confiscation of crime-related proceeds, instrumentalities and property, which provided for three possible approaches to Member States regarding the extended confiscation. The Directive obliges MS to regulate extended confiscation: when a court is **satisfied** that the property derived from **criminal conduct** for example if the value of property is disproportionate to the lawful income of a convicted person.  **Non-conviction (civil) confiscation**: While the Framework Decision **2005/212/JHA** in Article 3/4 provided for an option for Member States that **may use procedures other than criminal procedures** to deprive the perpetrator of the property in question, the Directive does not have such explicit provision any more, except in recital.10.  **Trainer should explain the national legal provisions regarding extended confiscation and/or civil confiscation – see the Warsaw Convention Article 3/4 and Directive 2014/42/EU Article 5?**  Directive 2014/42/EU Article 5 (Extended confiscation)  Member States shall adopt the necessary measures to enable the confiscation, either in whole or in part, of property belonging to a person convicted of a criminal offence which is liable to give rise, directly or indirectly, to economic benefit, where a **court, on the basis of the circumstances of the case, including the specific facts and available evidence, such as that the value of the property is disproportionate to the lawful income** of the convicted person**, is satisfied that the property in question is derived from criminal conduct**.  Warsaw Convention Article 3/4 Each Party **shall** adopt such legislative or other measures as may be necessary to require that, in respect of a serious offence or offences as defined by national law, an **offender demonstrates the origin** of alleged proceeds or other property liable to confiscation to the extent that such a requirement is **consistent with the principles of its domestic law**.  Note: according to the paragraph 4 of Article 53 the State may declare a reservation to the use of this provision.  **Framework Decision 2005/212/JHA** on confiscation of crime-related proceeds, instrumentalities and property (Article 3 Extended powers of confiscation)   1. Each Member State shall as a minimum adopt the necessary measures to enable it, under the circumstances referred to in paragraph 2, to **confiscate, either wholly or in part**, property belonging to a person **convicted of an offence** 2. committed within the framework of a **criminal organisation** as defined in Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union[(5)](http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32005F0212#ntr5-L_2005068EN.01004901-E0005), when the offence is covered by:   Council Framework Decision 2000/383/JHA (counterfeiting euro), Council Framework Decision 2001/500/JHA (**money laundering**, confiscation of proceeds), Council Framework Decision 2002/629/JHA (trafficking in human beings), Council Framework Decision 2002/946/JHA (unauthorised entry, transit and residence), Council Framework Decision 2004/68/JHA (child pornography), Council Framework Decision 2004/757/JHA drug trafficking.   1. which is covered by the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating **terrorism**   provided that the offence according to the Framework Decisions referred to above   * regarding offences other than **money laundering** are punishable with criminal penalties of a maximum of at least between 5 and 10 years of imprisonment, * regarding **money laundering**, are punishable with criminal penalties of a maximum of at least 4 years of imprisonment,   and the offence is of such a nature that it can generate financial gain.   1. Each Member State shall take the necessary measures to enable confiscation under this Article at least: 2. where a national court based on specific facts **is fully convinced** that the property in question has been **derived from criminal activities** of the **convicted person during a period prior** to conviction for the offence referred to in paragraph 1 which is **deemed reasonable** by the court in the circumstances of the particular case, or, alternatively, 3. where a national court based on specific facts is fully convinced that the property in question has been derived **from similar criminal activities** of the convicted person during a period prior to conviction for the offence referred to in paragraph 1 which is deemed reasonable by the court in the circumstances of the particular case, or, alternatively, 4. where it is established that the **value of the property is disproportionate to the lawful income** of the convicted person and a national court based on specific facts is fully convinced that the property in question has been derived from the **criminal activity** of that convicted person. 5. Each Member State may also consider adopting the necessary measures to enable it to confiscate, in accordance with the conditions set out in paragraphs 1 and 2, either wholly or in part, **property acquired by the closest relations** of the person concerned and property transferred to a **legal person** in respect of which the person concerned — acting either alone or in conjunction with his closest relations — has a controlling influence. The same shall apply if the person concerned receives a significant part of the legal person’s income.   4.   Member States **may use procedures other than criminal procedures** to deprive the perpetrator of the property in question. | |
|  | **Financial Investigation Elements: Management of frozen/confiscated property**  Note for trainer: This is a relevant topic for consideration, but needs to only be mentioned.  **The trainer should provide information to the students about the responsible authority and relevant rules on management of frozen/confiscated property. Powers to sell frozen property?**  Directive 2014/42/EU Article 10 (Management of frozen and confiscated property)   1. Member States shall take the necessary measures, for example by establishing centralised offices, a set of specialised offices or equivalent mechanisms, to ensure the adequate management of property frozen with a view to possible subsequent confiscation. 2. Member States shall ensure that the measures referred to in paragraph 1 include the possibility to sell or transfer property where necessary. 3. Member States shall consider taking measures allowing confiscated property to be used for public interest or social purposes.   **Warsaw Convention Article 6 (Management of frozen or seized property):** measures to ensure proper management of frozen or seized property. | |
| **Slide 26** | **Financial Investigation Elements: Data and Statistics**  It is important to keep the evidence and statistics on estimated value of property benefit/damage from criminal offence; on proposals for freezing orders; issued freezing orders; frozen property domestic and abroad; decisions on confiscation and value; executed confiscation; open claims to be executed; mutual legal assistance (legal basis (Warsaw Convention and other for: incoming/outgoing requests for bank data, freezing orders, frozen property, confiscation orders, confiscated property, asset sharing).  Such data is needed to monitor the implementation of freezing and confiscation of proceeds of crime, and to improve institutional and/or legal frameworks if the results are not as expected.  In some cases the obligation to report is established by international instruments and monitoring bodies, such as MONEYVAL or GRECO.  **Trainer should explain to students national situation concerning data kept on (legal basis):**   * financial investigation and value of property benefit/proceeds * freezing orders and value of frozen property (domestic and abroad) * management (and disposal) of frozen property * confiscation decisions and value * executed confiscation decisions and value * pending executions of confiscation decision * international cooperation – mutual legal assistance in access to bank data (account holder data, transactions and monitoring order), for freezing orders, confiscation orders and assets-sharing.     **Is your record centralised?**  If no, are relevant institutions (police, prosecution, courts, FIU) cooperating in gathering data and their presentation in e.g. yearly report?  Trainer should present the statistics in relation to number of criminal offences, number of money laundering offences and cybercrime offences.  Directive 2014/42/EU Article 11 (Statistics)   1. Member States shall regularly collect and maintain comprehensive statistics from the relevant authorities. The statistics collected shall be sent to the Commission each year and shall include: 2. the number of freezing orders executed; 3. the number of confiscation orders executed; 4. the estimated value of property frozen, at least of property frozen with a view to possible subsequent confiscation at 5. the time of freezing; 6. the estimated value of property recovered at the time of confiscation. 7. Member States shall also send each year the following statistics to the Commission, if they are available at a central level in the Member State concerned: 8. the number of requests for freezing orders to be executed in another Member State; 9. the number of requests for confiscation orders to be executed in another Member State; 10. the value or estimated value of the property recovered following execution in another Member State. 11. Member States shall endeavour to collect data referred to in paragraph 2 at a central level. | |
| **Slide 27-29** | Conducting financial investigations in parallel to criminal investigations requires interagency cooperation (prosecutor, units within the police – cybercrime unit, financial investigation unit, etc.) and Financial Intelligence Unit (FIU) in cases of money laundering.  It is important to understand the roles, responsibilities and powers of such agencies/units, according to national legislation, in order to be able to build on synergies of cooperation.  A cooperation protocol on practical issues might be considered to address questions like sharing information, information flow, division of tasks, forms like task force, joint investigation, regular meetings, etc.  Trainer should provide information on national situation concerning:   * Specialised units in the police/prosecutors office/courts * Financial investigation * Cybercrime * E-evidence (forensics) * Money laundering * Unit for management of frozen/confiscated property * Interagency cooperation under the lead of the prosecutor * Task force approach led by prosecutor, participation police, tax service, FIU, others (accounting, cyber experts etc.) * Relevant legal provisions for task force approach. | |
| **Slide 30** | Financial investigation and money laundering can have specific mutual interaction.  Criminal investigation and financial investigation can lead to the identification of money laundering typologies[[16]](#footnote-16) (techniques for concealing the origin of money) and therefore to the elements of criminal offence of money laundering. When such conditions are met, the FIU can be engaged and its powers can be invoked. In cases of cybercrime or online crime it is important to focus on possible elements of money laundering, including the typologies of money laundering online (see lessons on online criminal money flow typologies). In such cases the FIU can contribute with its analytical ability of financial (bank) data, as well as with speedy postponement of transactions, both domestically and internationally.  As mentioned in relation to the first element of financial investigations in this presentation, criminals tend to cover the source of criminal proceeds and to reinvest criminal profit to legal economy so during the financial investigation typologies of money laundering should also be observed.  The value of suspicious transactions is identified by FIU. With further analysis a link to predicate offences could be established, though it is not necessary to prove the link with a specific criminal offence. It is therefore not required to precisely identify and prove the value of criminal proceeds from a specific predicate offence. It is considered that the proceeds from a predicate offence become subject (instrumentality) of a money laundering offence (as discussed in relation to the second element of financial investigations in this presentation).  Also by analysing bank transactions and connections of suspect in case of money laundering, other relevant bank accounts and property can be discovered (as mentioned in relation to the third element of financial investigations in this presentation). Engagement of FIU could be most useful in case financial investigation shows the suspicion also of money laundering in addition to the (predicate) offence.  Apart of access of FIU to bank data domestically and abroad, and its analytical capability it is also important to take into account the power of FIU to timely postpone bank transactions both domestically and abroad. Such possibility can be considered in relation to the fourth element of financial investigations as discussed in this presentation.  This topic will be discussed in more detail in the lesson on FIUs. | |
| **Slide 31** | On the other hand, the anti-money laundering legislation provides for a series of prevention measures that enable the FIU to identify and analyse suspicious transactions that are reported by obliged institutions (banks, exchange offices and other entities). Based on such analysis, typologies of money laundering can be identified, which lead to the suspicion of money laundering by certain person or persons. In such cases, the prevention system can trigger, based on reports by banks and other entities and consequently by the FIU, a criminal investigation of a predicate offence by the police and prosecutor. This is particularly relevant in cases of online crime, including cybercrime, where timely reaction might be crucial to identify the criminal and to secure the crime proceeds.  In such cases the information of the FIU (intelligence) would be crucial to start the criminal and financial investigations. The temporary (administrative) postponement of a transaction by the FIU (nationally and internationally) would be complemented by court freezing order in criminal proceedings and request for mutual legal assistance in cross-border cases.  This topic is discussed in more detail in the lesson on the role of the FIU.  The trainer should use this slides to explain the interlinking relationship between the FIU role and the police/prosecutor role, as discussed above, FIU role involves monitoring and investigating suspicious transactions to identify money laundering activities. Criminal investigations and financial investigations pursue criminal activity and proceeds from crime. Proceeds from crime are typically laundered in some way, and laundered funds are in many cases used as in instrumentality to commit further crime. Therefore, the trainer should explain that as shown in this diagram, the work of the FIU and the police/prosecutors are closely linked together. | |
| **Slide 32** | Discuss domestic legal provisions and jurisprudence for:   * Financial investigation (report on FI, access to bank data – account, transactions, monitoring, use of special investigative methods (SIMS)) * Freezing of transaction/property * Confiscation of criminal proceeds * Extended confiscation * Money laundering offence   Provide/discuss template/forms for:   * Financial investigation (report on FI, access to bank data – account, transactions, monitoring, use of special investigative methods (SIMS)) * Freezing order and proposal * Confiscation decision (part of judgment?) and proposal * Extended confiscation * FIU order to bank to postpone financial transaction | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.1.4 – Introduction to Financial Intelligence Units and the Money Laundering Offence | | **Duration: 90 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 role and activity of financial intelligence units and also a basic description of the money laundering offence. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the functions, responsibilities and powers of a Financial Intelligence Unit (FIU) * Understand the types of information that an FIU has access to. * Know how FIUs exchange information. * Be aware of the relevant international standards. * Explain the basic nature of the money laundering offence. * Describe the relevance of money laundering to a financial investigation * Provide an example of how FIUs can help with cases involving online crime proceeds. | | |
| **Introduction:**  This session provides information on Financial Intelligence Units (FIUs) and money laundering, for those who have no familiarity with these topics.  All information about this session is included in the PowerPoint presentation entitled “Session 1.1.3 – Introduction to FIUs and ML” 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. | | |
| **Slide Notes** |  | |
| **Slide 2** | At the conclusion of this lesson, students should be aware of the reason an FIU exists, its role and responsibilities, what information a FIU has access to and how to request relevant information from a foreign and whether such information can be used as evidence in a prosecution. They will also be made aware of the international standards for anti-money laundering.  There is also a description of the money laundering offence and an explanation of the relationship between money laundering and financial investigations. | |
| **Slide 3** | The trainer should explain to the students what FIUs do and why countries have FIUs.  FIUs exist to receive and analyse reports on suspected money laundering. This is required by FATF Recommendation 29 which says that countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.  Reports on suspected money laundering are made as a suspicious transaction report ‘STR’ or suspicious activity report ‘SAR’ by the obliged entity or even an individual who comes to suspect money laundering. Bank account secrecy should not be an impediment to STR reports.  Obliged entity is a generic name given to the myriad of financial businesses that are obliged by law to comply with domestic AML regulations. The full list of types of businesses is described in the EU money laundering directives following the FATF recommendations and is reproduced here for convenience:   * credit institutions * financial institutions * the following natural or legal persons acting in the exercise of their professional activities: * auditors, external accountants and tax advisors * notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for the client concerning the * buying and selling of real property or business entities. * Managing of client money, securities or other assets * Opening or management of bank, savings or securities accounts * Organisation of contributions necessary for the creation, operation or management of companies * Creation, operation or management of trusts, companies, foundations or similar structures * Trust or company service providers not already covered under points (a) or (b) * Estate agents * Other natural or legal persons trading in goods, only to the extent that payments are made or received in cash in an amount of EUR10,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked * Providers of gambling services.   With the exception of casinos and following an appropriate risk assessment, Member States may decide to exempt fully or in part providers of certain gambling services from national provisions transposing the provisions of the Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.  FIUs may also receive Currency Transaction Reports where there is a requirement for travellers to declare sums in excess of €15000 in cash or negotiable instrument when crossing an EU border.  FIUs should analyse STR/CTR to determine if money laundering is apparent from the data and from cross checking other databases. Should the FIU reach an appropriate conclusion they will make a report to the police or prosecutor.  As can be seen here, FIUs are spilt roughly 50/50 between law enforcement and administrative FIUs. What does this mean in reality? Administrative FIU’s are often sited within a Ministry of Finance/Treasury or have a separate ‘agency’ status. They usually work in isolation from police of other law enforcement bodies and the FIU receives and analyses information received from banks and other obliged entities on suspected money laundering. The information is received in the form of suspicious activity reports (SAR) and possibly currency transaction reports (CTR).  **Administrative FIUs** are usually part of the structure, or under the supervision of, an administration or an agency other than the law-enforcement or judicial authorities. They sometimes constitute a separate agency, placed under the substantive supervision of a ministry or administration (“autonomous” FIUs) or not placed under such supervision (“independent” FIUs). The main rationale for such an arrangement is to establish a “buffer” between the financial sector (and, more generally, entities and professionals subject to reporting obligations) and the law-enforcement authorities in charge of financial crime investigations and prosecutions. Often, financial institutions facing a problematic transaction or relationship do not have hard evidence of the fact that such a transaction involves criminal activity or that the customer involved is part of a criminal operation or organisation. They will therefore be reluctant to disclose it directly to a law enforcement agency out of concern that their suspicion may become an accusation that could be based on a wrong interpretation of the facts. The role of the FIU is then to substantiate the suspicion and send the case to the authorities in charge of criminal investigations and prosecutions only if the suspicion is substantiated.  Examples: Andorra, Aruba, Australia, Belgium, Bolivia, Bulgaria, Canada, Columbia, Croatia, the Czech Republic, France, Israel, the republic of Korea, Liechtenstein, Malta, Monaco, the Netherlands, the Netherland Antilles, Panama, Poland, Romania, Russia, Slovenia, Spain, Ukraine, the United States and Venezuela.  **Law Enforcement FIUs**. In some countries, the emphasis on the law-enforcement aspects of the FIU led to the creation of the FIU as part of a law-enforcement agency, since this was the easiest way to establish a body with appropriate law enforcement powers without having to design from scratch a new entity and a new legal and administrative framework. Operationally, under this arrangement, the FIU will be close to other law enforcement units, such as a financial crimes unit, and will benefit from their expertise and sources of information. In return, information received by the FIU can be accessed more easily by law enforcement agencies and can be used in any investigation, thus increasing its usefulness. Exchange of information may also be expedited through the use of existing national and international criminal information exchange networks.  **Judicial or prosecutorial-type FIUs**. This type of FIU is established within the judicial branch of the state and most frequently under the prosecutor’s jurisdiction. Instances of such an arrangement are found in countries with a continental law tradition, where the public prosecutors are part of the judicial system and have authority over the investigative bodies, allowing the former to direct and supervise criminal investigations. Disclosures of suspicious financial activity are usually received by the prosecutor’s office, which may open an investigation if suspicion is confirmed by the first inquiries carried out under its supervision. The judiciary’s powers (e.g. seizing funds, freezing accounts, conducting interrogations, detaining suspects and conducting searches) can then be brought into play without delay. Judicial and prosecutorial FIUs can work well in countries where banking secrecy laws are so strong that a direct link with the judicial or prosecutorial authorities is needed to ensure the cooperation of financial institutions. It may be noted that the choice of the prosecutor’s office as the location of an FIU does not exclude the possibility of establishing a police service with special responsibility for financial investigations. Also, in many countries, the independence of the judiciary inspires confidence in financial circles. The principal advantage of this type of arrangement is that disclosed information is passed from the financial sector directly to an agency located in the judiciary for analysis and processing.  Examples: Austria, Estonia, Germany, Guernsey, Hungary, Iceland, Ireland, Jersey, Slovakia, Sweden and the United Kingdom.  **Hybrid FIUs**. This hybrid type of arrangement is an attempt to obtain the advantages of all the elements put together. Some FIUs combine the features of administrative-type and law-enforcement-type FIUs, while others combine the powers of the customs office with those of the police. For some countries, this is the result of joining two agencies that had been involved in combatting money laundering into one. It may be noted that in some FIUs listed ad administrative-type, staff from various regulatory and law enforcement agencies work in the FIU while continuing to exercise the powers of their agency of origin. Amongst the countries that have established “hybrid” FIUs are Denmark, Jersey, Guernsey and Norway.  Examples: Luxembourg, Cyprus.  Not all FIUs confine themselves to money laundering offences. Financial information can often lead to the detection of other criminal offences. | |
| **Slide 4** | The trainer will explain that FIUs, to fulfil their functions, need access to as many relevant databases as possible. As explained earlier there are different models of FIU and to some extent this governs the nature of potential database access. Law enforcement FIUs usually have immediate access to police databases, criminal records, vehicle registrations, etc. Administrative FIUs usually only gain access to police databases upon request, or possible through an attached police liaison officer.  All FIUs need access to property (cadastral) and business databases. Many FIUs buy access to commercial credit reference agency databases. Some countries keep registers of bank accounts and FIUs should have access to these or may even be obliged to maintain such registers. It is a recommendation of the EU 4th Anti Money Laundering Directive that EU countries consider establishing such a register. | |
| **Slide 5** | FIUs may have powers to temporarily freeze bank accounts, usually on administrative grounds as a delayed transaction (in effect a freeze) on their own powers pending a court/prosecutors Order. This is usually where money laundering is concretely suspected and the balance of an account may be paid away thus allowing a criminal to successfully launder his money. Accounts can also be frozen in an emergency to frustrate any attempts to pay away proceeds that might be subject to a Confiscation Order.  FIU powers to delay transactions from bank accounts or transactions are usually time limited and meant to preserve the status quo whilst formal Court Orders are obtained. The exact process and time limits vary from country to country.  The corollary of delaying transactions is that sometimes explicit authority may need to be granted by the FIU to an obliged entity to continue a transaction which may constitute money laundering. The term used is ‘to seek consent’.  Some FIUs, such as those with a responsibility to oversee compliance with AML/CFT laws/regulation, have the authority to issue administrative sanctions (usually a penalty/fine) where they believe an regulated entity is failing to properly discharge its compliance with AML/CFT regulations. | |
| **Slide 6** | The trainer should ensure that the students know their country arrangements for their FIU.  They should know how to communicate and know the likely range of information held by their FIU. Not every FIU receives CTRs whilst all will receive SARs. Some FIUs (e.g. France) may hold a register of bank accounts. Depending on the nature of the FIU it may have access to law enforcement databases, vehicle and cadastral registers, social and welfare databases, customer credit information, bank account data. Trainer should familiarise themselves with the possibilities of their own FIU.  CTRs are made to an FIU (where legislated for) when a cash transaction meets or exceeds a threshold. For example in the USA it was $10,000, but widespread placements of just under the limit resulted in the USA monitoring lower amounts to detect ‘structuring’ often known as **smurfing**, this is a method of placement\* whereby cash is broken into smaller deposits of **money**, used to defeat suspicion of **money laundering** and to avoid **anti**-**money laundering** reporting requirements.  In the EU, the 3rd Anti-Money Laundering Directive imposed a requirement to declare cash currency at borders where cash or monetary instruments exceeded €15,000 in value. The subsequent reports are forwarded to the FIU.  If you are making an enquiry of an FIU you should have the basic requirements prepared such as the suspect’s details, nature of offence and brief outline of case. On a human rights point it should be noted that SARs are the manifestation of a subjective untested suspicion by the reporter and not backed by a grounded suspicion or intelligence and so should be regarded as such unless reinforced by objective intelligence or evidence. This approach lies at the heart of the Egmont Group principles of information exchange.  Egmont Group is the name of the ‘club’ of FIUs named after the Palace of Egmont in Brussels where the founding agreement for FIUs was made to cooperate and exchange information in 1995. In 2007 the Egmont Group proclaimed itself with a Charter and established itself as a recognised international organisation. Egmont Group is funded through a levy on each member FIU based on a formula determined by their nation’s GDP output.  The Egmont Group Statement of Principles of information exchange requires for one FIU to ask of one or more FIUs to exchange information relevant to its duties the following principle should be applied (next slide)  \*The classical money laundering process has been broken down into 3 descriptors to complete the process.  1. PLACEMENT – the cash is ‘placed’ into the financial system. This usually means achieving the cash to non-cash (e.g. placed into a bank account at its most simplest) economy. This is a crucial stage where interdiction can be most effective.  2. LAYERING – moving the money from account to account from jurisdiction to jurisdiction, washing it through tax havens etc to place ‘layers’ of obfuscation between the start of the laundering process (placement) and the final stage which is…..  3. INTEGRATION. At this point the launderer has achieved their objective. The criminal proceeds have been integrated into the legitimate economy and the criminal can enjoy the fruits of his crimes. | |
| **Slide 7** | The trainer should expand on the bullet points and elaborate on the text below:  ***A. General Framework***  International co-operation between FIUs should be encouraged and based upon a foundation of mutual trust.    FIUs should take steps to seek information that may be used by other, identified, domestic law enforcement or financial supervisory agencies engaged in enforcement and related regulatory activities.    FIUs should work to encourage that national legal standards and privacy laws are not conceived as to inhibit the exchange of information, in accordance with these principles, between or among FIUs.  Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.    ***B. Conditions for the Exchange of Information***    FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party. Such exchange, either upon request or spontaneously, should produce any available information that may be relevant to an analysis or investigation of financial transactions and other relevant information and the persons or companies involved.    An FIU requesting information should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the receiving FIU to determine whether the request complies with its domestic law.    ***C. Permitted Uses of Information***    Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.    The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information.    ***D. Confidentiality – Protection of Privacy***    All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with national provisions on privacy and data protection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU. | |
| **Slide 8** | Trainers notes Egmont Group continued:  If you ask your FIU to request an Egmont Group FIU-FIU search for information you must be specific which FIU(s) you want your FIU to make a request of. Egmont Group principles do not allow for general fishing for information. If you have grounded intelligence that your suspect may have a bank account in the requested country then say so, or perhaps he/she frequently travels to the requested country or may own property there (consider Camden Assets Recovery Interagency Network (CARIN)/ ARO requests). | |
| **Slide 9** | The trainer will explain that  Egmont Group Secure Web (ESW);  Under the Egmont Group umbrella, all FIUs that are members have access to the Egmont Secure Web. This is a secure communications channel and is used to make a request of another FIU. Over recent years extra functionality has been added to provide bulletin board and joint working areas where FIUs can cooperate on joint analysis or investigations. ESW is provided and maintained by FinCEN, the FIU of the USA.  FIU.net is another secure communications facility provided by the EU to link EU FIUs exclusively. It holds no data itself (unlike ESW) all data is held within the host FIU but allows collaborative working on joint investigations or analysis. FIU.net has also trialled bulk data comparison using anonymised FIU data to compare with other FIUs participating in the experiment. There has been some success in identifying same suspects occurring in different FIU databases. Although not described as ‘fishing’ this tool allows targeted FIU-FIU requests on hitherto unknown links. The main downside is over-retrieval of common anonymised data links which need human intervention to bottom out. FIUs rarely have enough resources to do this.  How can you use information from an FIU? It is rare that an FIU in another country would allow its information to be used in a prosecution without further request, usually a Mutual Legal Assistance request. It is one of the Egmont Group Principles that any information supplied to you (from a foreign FIU) can only be used for the purposes for which it was requested (and articulated in the request).  FIU information is however, usually only a pointer or indicator to a financial institution or individual who could be approached directly to obtain evidence. If an FIU enquiry reveals the existence of a relevant bank account then the necessary order (in domestic enquiries) can be made. In international enquiries an MLA to the appropriate Central Authority for the requested country can be made.  CARIN (Camden Asset Recovery Information Network) and ARO (Asset Recovery Offices) are sometimes to be found hosted by the FIU. These are not specific FIU bodies but are concerned with providing informal (CARIN) or formal (ARO) assistance on identifying and tracing assets liable to criminal confiscation measures. It is a matter for each jurisdiction how they structure these offices. There is further information on CARIN and ARO in the topic on informal and formal information exchange and Mutual Legal Assistance. | |
| **Slide 10** | The trainer will explain that that some FIUs, usually of an Administrative nature, are also given supervisory responsibilities to train and supervise obliged entities\* in their compliance with domestic money laundering regulations. The FIU may offer training programmes for staff of obliged entities in their regulated sector in compliance programmes to counter money laundering.  FIUs should also develop money laundering typologies to assist their regulated sector in enhancing AML awareness and improve the quality of SAR/STRs.  \*Obliged entity is a generic name given to the myriad of financial businesses that are obliged by law to comply with domestic AML regulations. The full list of types of businesses is described in the EU money laundering directives following the FATF recommendations and is reproduced here for convenience:-  (1) credit institutions;  (2) financial institutions;  (3) the following natural or legal persons acting in the exercise of their professional activities:  (a) auditors, external accountants and tax advisors;  (b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the:  (i) buying and selling of real property or business entities;  (ii) managing of client money, securities or other assets;  (iii) opening or management of bank, savings or securities accounts;  (iv) organisation of contributions necessary for the creation, operation or management of companies;  (v) creation, operation or management of trusts, companies, foundations, or similar structures;  (c) trust or company service providers not already covered under points (a) or (b);  (d) estate agents;  (e) other natural or legal persons trading in goods, only to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;  (f) providers of gambling services.  With the exception of casinos and following an appropriate risk assessment, Member States may decide to exempt fully or in part providers of certain gambling services from national provisions transposing the provisions of this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.  National Risk Assessment: In 2012 the FATF issued a list of revised recommendations to counter money laundering and counter terrorist finance (CFT). It also revised the methodology through which mutual evaluations of compliance with FATF recommendations are conducted. Hitherto the methodology consisted chiefly of an assessment of relevant legislation to ensure that the jurisdiction had the necessary legal structures. The new methodology concentrates on the evaluation of effectiveness of AML/CFT legislation and its use.  Underpinning this is new recommendation 1: Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.  This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions. Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.  Most countries rely heavily upon the FIU to either conduct the risk assessment or to contribute to large parts of it. It cannot be stressed too much how important that a meaningful Risk Assessment is conducted and then this is seen to drive AML/CFT activity in response. The R.A. should not be a regurgitation of all possible AML/CFT risks but should be driven by intelligence and operational experience into the actual risks most apparent in your country. To do this it is important that law enforcement in particular, including FIUs, understand the nature of organised crime (OC) in their country, the drivers and enabling factors that allows OC and corruption to operate and flourish and how law enforcement and Government can create a hostile environment to OC. One of the key weapons against OC/corruption is effective asset/proceeds of crime confiscation. | |
| **Slide 11** | As described in the notes to slide 6, the classical money laundering process has been broken down into 3 descriptors to complete the process.  1. PLACEMENT – the cash is ‘placed’ into the financial system. This usually means achieving the cash to non-cash (e.g. placed into a bank account at its most simplest) economy. This is a crucial stage where interdiction can be most effective.  2. LAYERING – moving the money from account to account from jurisdiction to jurisdiction, washing it through tax havens etc to place ‘layers’ of obfuscation between the start of the laundering process (placement) and the final stage which is…..  3. INTEGRATION. At this point the launderer has achieved their objective. The criminal proceeds have been integrated into the legitimate economy and the criminal can enjoy the fruits of his crimes.  There are many variants to this process and for many launderers the placement level, i.e. bridging the cash to non-cash hurdle has already been achieved, especially in many cybercrime scenarios where bank account contents are stolen or a victim of ransomware pays through a virtual currency. Once the proceeds of the crime are in electronic form the hardest part of a launderers job has been overcome.  FIUs can help jurisdictions through the development of typologies of money laundering as it is perceived in your State. The FATF website also regularly publishes ML typologies.  This 3-stage process is shorthand for the money laundering process. The international conventions go further in describing the types of activity that should be criminalised  Recognising the pernicious aspects of money laundering and its effect on economies and understanding that organised crime can only be defeated through identifying and wherever possible punishing and removing launderers from supporting and enabling organised crime (and acquisitive crime in general), the international community has developed a framework of anti-money laundering standards enshrined in the Conventions shown in the slide. The **FATF recommendation 3** also requires the criminalisation of money laundering in member jurisdictions as described on the Palermo and Vienna Conventions.  The Council of Europe **‘Warsaw’ Convention** (CETS 198) Article 9 proscribes the ML offence thus:-  1 Each Party shall adopt such legislative and other measures as may be necessary to establish as offences under its domestic law, when committed intentionally:  a the conversion or transfer of property, knowing that such property is proceeds, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions;  b the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is proceeds;  and, subject to its constitutional principles and the basic concepts of its legal system;  c the acquisition, possession or use of property, knowing, at the time of receipt, that such property was proceeds;  d participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.  2 For the purposes of implementing or applying paragraph 1 of this article:  a it shall not matter whether the predicate offence was subject to the criminal jurisdiction of the Party;  b it may be provided that the offences set forth in that paragraph do not apply to the persons who committed the predicate offence;  c knowledge, intent or purpose required as an element of an offence set forth in that paragraph may be inferred from objective, factual circumstances.  3 Each Party may adopt such legislative and other measures as may be necessary to establish as an offence under its domestic law all or some of the acts referred to in paragraph 1 of this Article, in either or both of the following cases where the offender  a suspected that the property was proceeds,  b ought to have assumed that the property was proceeds.  4 Provided that paragraph 1 of this article applies to the categories of predicate offences in the appendix to the Convention, each State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that paragraph 1 of this article applies:  a only in so far as the predicate offence is punishable by deprivation of liberty or a detention order for a maximum of more than one year, or for those Parties that have a minimum threshold for offences in their legal system, in so far as the offence is punishable by deprivation of liberty or a detention order for a minimum of more than six months; and/or  b only to a list of specified predicate offences; and/or  c to a category of serious offences in the national law of the Party.  5 Each Party shall ensure that a prior or simultaneous conviction for the predicate offence is not a prerequisite for a conviction for money laundering.  6 Each Party shall ensure that a conviction for money laundering under this Article is possible where it is proved that the property, the object of paragraph 1.a or b of this article, originated from a predicate offence, without it being necessary to establish precisely which offence.  7 Each Party shall ensure that predicate offences for money laundering extend to conduct that occurred in another State, which constitutes an offence in that State, and which would have constituted a predicate offence had it occurred domestically. Each Party may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.  One of the key points of Article 9 (2) is that the Court does not have to necessarily prove a predicate offence, it is sufficient to show that these are proceeds of a crime and that the defendant knew this. Sometimes referred to as the ‘stand–alone money laundering offence’.  The UN **Palermo Convention** on Transnational and Organised Crime (2000) Article 6 criminalises money laundering in similar terms to the **Warsaw Convention** thus:   1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:   *(a)* (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;  (ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;  *(b)* Subject to the basic concepts of its legal system:  (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;  (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.  2. For purposes of implementing or applying paragraph 1 of this article:  (*a*) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences;  (*b*) Each State Party shall include as predicate offences all serious crime as defined in article 2 of this Convention and the offences established in accordance with articles 5, 8 and 23 of this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in such list a comprehensive range of offences associated with organized criminal groups;  (*c*) For the purposes of subparagraph *(b),* predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and  would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;  *(d)* Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;  *(e)* If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;  *(f)* Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.  Article 7 of the **Palermo Convention** requires States to implement a regulatory and supervisory regime to detect and counter money laundering in the financial sector. This Article also calls for States to create an FIU as part of these structures.  The 1988 UN **Vienna Convention** on against illicit traffic in narcotic drugs and psychotropic substances Article 3(1)(b) criminalised the transfer of property from crime thus:  i) The conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with subparagraph *a)* of this paragraph, or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;  ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with subparagraph *a)* of this paragraph or from an act of participation in such an offence or offences;  Property as defined in Article 1 (q) means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.  Money laundering is a multi-headed hydra and as jurisdictions impose tighter regulatory environments then launderers resort to ever more imaginative methods. The last 10 years has seen increased use of money brokers who play an increasing role in the laundering of the proceeds of organised crime. These brokers arrange for cash to be collected from organised crime groups, usually by anonymous ‘collectors’. The broker arranges for the value represented to be paid wherever the organised crime group requires. In the example of the sale and distribution of cocaine this is often done on credit by the Colombian cartels. Once the importer of the cocaine pays over the money to the brokers’ collector, the payment is made instantly to the cartels thus removing risk from the importer of interdiction (cash seizures) by law enforcement. Any loss is carried by the broker. The ‘collector’ pays in the cash typically to a Bureau Exchange who then wires the money to an account in UAE where it is removed in cash thus breaking the audit trail. The Bureau will submit a SAR covering the transaction but this is of little use as the ‘collector’ will never be seen again.  It is an important aspect of the National Risk Assessment (FATF R.1) that authorities understand the characteristics of money laundering in their jurisdiction. What are the enabling features that contribute or facilitate money laundering in your country? What can be done to remedy this? | |
| **Slide 12** | The trainer will explain that the Financial Action Task Force (FATF) sets the international standards on combating money laundering and the financing of terrorism and proliferation.  The FATF is an inter-governmental body established in 1989 by the Ministers of the then G7 countries. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system.  In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse. The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.  Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:   * identify the risks, and develop policies and domestic coordination; * pursue money laundering, terrorist financing and the financing of proliferation; * apply preventive measures for the financial sector and other designated sectors; * establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures; * enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and * facilitate international cooperation.   The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).  Following the conclusion of the third round of mutual evaluations of its members, the FATF reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs e.g. The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL for Europe) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.  The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced.  Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way. | |
| **Slide 14** | Financial investigation and money laundering can have specific mutual interaction.  Criminal investigation and financial investigation – can lead to the money laundering typologies for concealing the origin of money – and therefore to the elements of criminal offence of money laundering. When such conditions are met, the FIU can be engaged and its powers can be evoked.  As mentioned in the lesson on financial investigations – criminals tend to cover the source of criminal proceeds and to reinvest criminal profit to legal economy – so during the financial investigation typologies (techniques) of money laundering should also be observed.  FIUs should develop typologies of money laundering in their jurisdiction. This should reflect the typologies of actual cases and therefore the FIU should cooperate with law enforcement and prosecutors to identify salient features of money laundering cases and how it manifested itself. The FATF website hosts many generic typologies to assist FIUs and other institutions to identify money laundering.  The value of suspicious transactions is clarified by FIU analysis and their link to predicate offences could be looser, which allows for efficient establishment of value of criminal profit (which can assist with a financial investigation aiming to seize/confiscate crime proceeds).  Also by analysing bank transactions and connections of suspect in case of money laundering, other relevant bank accounts and property can be discovered (which can also assist with the financial investigation aiming to seize/confiscate crime proceeds). Engagement of FIU could be most useful in case financial investigation shows the suspicion also of money laundering besides the (predicate) offence.  Apart from access of FIU to bank data domestically and abroad, and its analytical capability it is also important to take into account the power of FIU to timely freeze the bank transaction both domestically and abroad. Once again, such possibilities should be considered in the framework of a financial investigation aiming to seize/confiscate crime proceeds. The use of an FIU’s power to freeze bank transactions can be used to prevent the transfer of crime proceeds outside the jurisdiction and/or otherwise out of the reach of the authorities.  The administrative money laundering preventive measures, conducted by FIU - can lead to the investigation into criminal offence of money laundering and also to discover the predicate offence/perpetrator. | |
| **Slide 15** | The interaction between a financial investigation and the FIU should be taken into account and benefits explored. However it depends on national legislation and jurisprudence (relevant judgments?)on necessary elements for criminal offence money laundering. And also on the status and powers of financial intelligence unit (FIU).  The trainer should guide a discussion with the students covering this and also the following questions:   * In practice, is the result of a Financial Investigation a money laundering charge? * Can the money laundering charges be more efficient than charging for predicate offence? Question of evidence! * What are the relevant ML typologies in similar (predicate) offences in practice? * Can FIU data be used as evidence in court criminal proceedings?   Because FIUs hold data usually submitted as a STR/SAR its reliability is untested. STRs represent the subjective suspicion of the reporter and as such may be of undetermined value. STRs in the context of an investigation (relevant to the defendant/s) are usually regarded as privileged information and there may be legislation that defines the status of STR material similar to that from a confidential informant. Even the existence of a STR is usually not disclosed.  However, STR material is usually a pointer to a bank account or financial institution from which evidence can be directly obtained in the usual way. In certain cases FIU analysts have given evidence of their conclusions in analytical reports to Police or prosecutors showing how financial transactions separately evidenced demonstrate money laundering activities. | |
| **Slide 17** | The trainer should briefly explain the “Business Email Compromise” fraud. | |
| **Slide 18** | The trainer should provide an explanation of how an FIU can help in such cases, in particular the trainer should emphasise the time critical nature of the interventions that can be made by the FIU. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.1.5 – Identifying Suspects on the Internet | | **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 * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Aim:** To provide the delegates with information about the relationship between an individual’s online activity and their real world identity, and some of the challenges associated with creating that link. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain important Internet terminology * Describe what is an IP Address * Describe how can you find a suspect IP address * Describe how can you associate a suspect IP address with a real person * List three technical challenges to identification of suspects on the Internet. | | |
| **Introduction:**  This session provides information on the identification of suspects online and the association of an individual’s online activity with their real world identity, as well as describing some of the challenges of creating that association.  All information about this session is included in the PowerPoint presentation entitled “Session 1.1.5 – Identifying Suspects on the Internet” 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. | | |
| **Slide Notes** |  | |
| **Slide 4** | The trainer should explain that the Internet is a global network. Operating any form of global infrastructure will necessarily be hugely technically complex. The purpose of this section is to introduce the basic terminology. The slides have been carefully prepared to simplify but not distort the relevant concepts. | |
| **Slide 5** | Communication protocols are used to standardise the structure of the data sent by the computers connecting to the network. Communication protocols are essential so that the computer receiving the data can interpret the incoming traffic. | |
| **Slide 7** | Describe the situation as follows:  There is a head office and two regional offices.  The offices are connected together by leased lines, leased from a telecommunications provider.  Question 1: In which of the following scenarios will information be transferred across the leased line?  a. Suppose there are two computers in the head office that communicate with each other.  In this case, the two computers are connected to the same local network, so information will not be transferred across the leased line.  b. Suppose there is a computer in the first regional office that wants to communicate with another computer in the first regional office.  In this case, the two computers are connected to the same local network, so information will not be transferred across the leased line.  c. Suppose there is a computer in the first regional office that wants to communicate with a computer in the head office.  In this case, the information will be transferred across the leased line, and then across the local network in the head office to the relevant computer.  d. Suppose there is a computer in the first regional office that wants to communicate with a computer in the second regional office.  In this case, the information will be transferred across the leased line from the first regional office to the head office, and then forwarded again from the head office to the second regional office.  Trainer should reinforce with the students that this is the key difference between a local area network and a wide area network. | |
| **Slide 8** | Bandwidth: Explain that bandwidth is usually measured in kilobits (thousands of bits) or megabits (millions of bits) per second.  Router: Refer back to the diagram on the previous page and point out the routers. Explain that the routers are the actual piece of networking hardware that decides whether or not to send the traffic along the leased line or not.  Switch: Explain that hubs (and in the vast majority of cases, switches) are what are at the other end of the wire that connects to your PC in work. These devices forward traffic to other PCs connected to the same local network.  NIC: Explain that this where the wire attaches in the back of your PC, in the case of a wired network or the piece of hardware that sends or receives radio waves in the case of a wireless network.  MAC address: Explain that this is used to uniquely identify computers on the local network but is only available on the local network and, generally speaking, cannot be used to identify people remotely.  Server: Explain that not all computers connected to a network are PCs with people sitting in front of them. Some services are provided by computers, and those computers are also connected to the network. For example, a web server, an email server and a file sharing server will all be connected to the network. From the point of view of the network, it doesn’t matter what the role of the computer is – whether it is a PC or a server – the same techniques are used for transferring information from one computer to another. However, it is important to understand that not all computers on a network are necessarily a PC or laptop with an individual sitting in front of them. | |
| **Slide 9** | Trainer should pose the question on the slide and ask participants for input. Explain that one option is that the two organisations could get a leased line between each other and use a model similar to the one described previously.  Trainer should indicate that this is indeed done at times but explain that this quickly becomes infeasible when hundreds of organisations want to form similar connections. Trainer should pose the rhetorical question, what if every organisation needed to get a leased line connection to Google in order to use their web search? What if they then wanted to talk to Microsoft, Amazon, Twitter, Linkedin, etc. Trainer should then explain that a much more sensible approach is to share a common communication infrastructure that has the capacity to forward traffic to the relevant locations, rather than each organisation getting a leased line to every other organisation that they might hypothetically want to talk to. In this scenario, Google and others are connected to a shared communication infrastructure and all that our hypothetical organisation needs to do is also connect to the shared infrastructure. Traffic destined for Google that is sent to the shared communication infrastructure will be forwarded to Google without the organisation needing to know exactly how to get traffic to this, or any other, particular destination.  This is the basis of the Internet. | |
| **Slide 10** | Trainer should explain that the idea of using a shared communication infrastructure brings up another question, how does the shared infrastructure know how to get information from any source to a particular destination. For example, how will the shared infrastructure know how to get information from our organisation to Google? Trainer should use the specific example of suppose you want to send a request to Google for the Google search page.  The answer is that Google, and all other possible communication parties on the shared infrastructure, need a uniquely identifying address. Similarly, when Google is sending the information back to our organisation, we will also need a uniquely identifying address so that the shared infrastructure knows where to send the response from Google. In other words, Google receives the request that you sent for the search page, where does Google send the response back to.  Explain that there are many different ways to answer this question, but in the case of the Internet, each communication party must be addressable by a unique address, known as an Internet Protocol or IP address. The job of the shared network infrastructure then becomes sending information to/from specific IP addresses – ultimately this is the job of the Internet. | |
| **Slide 11** | Trainer should explain that the Internet works by forwarding traffic from one IP address to another. Trainer should use this slide to explain the forwarding of traffic via various intermediary networks to the ultimate destination. Trainer should also explain that the response might not necessarily return to the sender along the same path that the request was sent.  Trainer should point out the two IP addresses on the slide and state that these are IP addresses. | |
| **Slide 12** | Trainer should explain that IP version 4 is still very commonly used, although there is a newer version of IP, called version 6, that is also deployed on the Internet. | |
| **Slide 13** | Trainer should remind students that the Internet is much more complex than we can possibly hope to cover in a short introduction like this. Trainer should caution students that there is not a simple one-to-one mapping between every person in the world and an IP address on the Internet.  Trainer should explain that IP addresses are typically traceable to a specific Internet service provider and may indeed be traceable to a specific geolocation. However, this information is not always accurate and there are all sorts of reasons why inaccuracy might arise. For example, if an Internet service provider sub-leases a portion of their IP addresses to another internet service provider they might not know how those IP addresses are being allocated to individual users.  There are many reasons why an IP address does not necessarily identify a specific individual (it is a necessary but not sufficient piece of Information).  Two specific examples should be discussed:   1. Static versus Dynamic IP addresses – Trainer should ask students to consider the case of their Internet connection at home. Most likely they either use a cable Internet provider or a DSL provider. In both cases, the trainer should explain, that the Internet Service Provider might, and most probably will, periodically change their IP address. This means that it’s important to not only know what IP address was in use, but also WHEN the IP address was in use to be able to identify a particular subscriber. A similar thing can happen within organisations – each time a PC is rebooted it might get a different IP address. 2. Network address translation – Trainer should explain that despite the fact that there are 4 billion available IP addresses, they are not allocated one by one, rather they are allocated in groups. One a group has been allocated to an organisation, no other organisation can use any IP address in that group. Trainer should explain that this leads to very inefficient allocation of IP addresses and therefore there is a problem with available IP addresses running out. Trainer should explain that this, amongst other reasons, has led to the need for a revised version of IP including longer addresses (IP version 6). Trainer should explain that there are certain groups of IP addresses that are not allowed to be used on the Internet. In other words, they will not be forwarded by the shared network infrastructure. Trainer can give the examples of any IP address starting with 10, or any IP address starting with “192.168”. Trainer should explain that these IP addresses can be used perfectly well on a local network, but not on the Internet. Trainer should explain that these IP addresses are used to make more efficient use of the available IP addresses in the following way:    1. Within the organisation, each PC is given an IP address that cannot be used on the Internet.    2. The organisation has a small number, perhaps just one, real Internet IP address assigned to it.    3. Whenever a PC wants to communicate with another computer on the Internet, the organisation’s infrastructure (Internet gateway router in particular) substitutes the real internet IP for the internal IP address before forwarding the traffic out to the Internet.    4. This allows a large number of PCs share a single IP address for communicating on the Internet, and the technique is known as Network Address Translation (NAT).   The upshot of the use of this technique, however, is that all of the PCs inside the organisation appear to the rest of the Internet as if they are a single computer with a single IP address. If this IP address is identified as part of an investigation, it is only the organisation itself that is in a position to determine which internal PC generated the traffic in question. | |
| **Slide 14** | Trainer should conduct an exercise where the students can find out their own IP address (e.g. ipconfig on a windows PC) and use online services such as whatsmyip.com, whatsmyip.org etc. to find out what their Internet-facing IP address is.  In cases where the training is being conducted on a private IP network, this is a useful way to further emphasise the nature of private vs. Internet IP addresses. | |
| **Slide 15** | This section of the course explains how it can be possible to associate an IP address with some suspicious activity online. This is a necessary component of an Internet based investigation. | |
| **Slide 17** | Trainer should explain that web servers will typically keep a record of all incoming requests.  Trainer should also explain, however, that this is a configuration option in a web server and a person who is running a web server can switch off the logging and may well do this if they are attempting to conceal the activity of the people using the web server. This will mean that no logs of the web browsing activity will be kept. | |
| **Slide 18** | The trainer should explain that this is an example of a web server log. Trainer should refer to the highlighted log entry and point out:   1. The source IP address – 216.128.130.126 2. The time/date of the HTTP request – 23/Sep/2006:21:30:02 -0400 – Trainer should point out the timezone, in this case GMT-4. 3. The thing that was requested “/pgp/” – this is known as the resource and will have meaning in the context of the server that is handling the request. It might be a document on the server, a folder on the server or an image, for example. 4. The page the user was on when they clicked on the link that led to this request. This is known as the referrer. In this case the long string starting with dir.yahoo.com. From this we can tell that the user was looking at this page, clicked on a link that led to this server receiving a request for a resource named “/pgp/”. 5. The browser identification string (starting Mozilla/4.0), which is provided by the browsing software of the client PC, although this can be faked/changed. | |
| **Slide 19** | Trainer should explain that unlike web browsing, the sender and recipient of an email do not interact directly. | |
| **Slide 21** | Trainer should explain that SMTP (Simple Mail Transfer Protocol) is the process by which email is sent and forwarded, POP (Post Office Protocol) or alternatively IMAP is the process by which email is checked/received.  Trainer should talk through the process of delivering an email via an outgoing mail server and an incoming mail server.  Trainer should explain that in the case of web-based email (e.g. gmail) that instead of using POP3 to interface with the incoming mail server, that the user logs in to a web server and reads the email directly on the incoming mail server. | |
| **Slide 23** | Trainer should explain that, although the students might not recognise email in this format, each email that have ever read has headers like this.  Trainer should highlight in particular   1. The Received headers, which show IP addresses that processed this email 2. The from and to email addresses 3. The subject 4. The Date   Trainer should point out that it is possible for some of this information to be faked if someone is trying to conceal the source of the email and therefore email header analysis requires some technical skill to interpret correctly. | |
| **Slide 24** | Trainer should ask the students to think of other services that might have IP addresses.  Trainer should stimulate discussions with examples such as Skype, Pokemon Go, DropBox, Facebook, Google, Microsoft. Etc. | |
| **Slide 25** | This section of the course explains how it can be possible to associate an IP address with some suspicious activity online. This is a necessary component of an Internet based investigation. | |
| **Slide 26** | Trainer should remind students that the Internet is much more complex than we can possibly hope to cover in a short introduction like this. Trainer should caution students that there is not a simple one-to-one mapping between every person in the world and an IP address on the Internet. There are many reasons why an IP address does not necessarily identify a specific individual (it is a necessary but not sufficient piece of Information).  Two specific examples should be discussed:   1. Static versus Dynamic IP addresses – Trainer should ask students to consider the case of their Internet connection at home. Most likely they either use a cable Internet provider or a DSL provider. In both cases, the trainer should explain, that the Internet Service Provider might, and most probably will, periodically change their IP address. This means that it’s important to not only know what IP address was in use, but also WHEN the IP address was in use to be able to identify a particular subscriber. A similar thing can happen within organisations – each time a PC is rebooted it might get a different IP address. 2. Network address translation – Trainer should explain that despite the fact that there are 4 billion available IP addresses, they are not allocated one by one, rather they are allocated in groups. One a group has been allocated to an organisation, no other organisation can use any IP address in that group. Trainer should explain that this leads to very inefficient allocation of IP addresses and therefore there is a problem with available IP addresses running out. Trainer should explain that this, amongst other reasons, has led to the need for a revised version of IP including longer addresses (IP version 6). Trainer should explain that there are certain groups of IP addresses that are not allowed to be used on the Internet. In other words, they will not be forwarded by the shared network infrastructure. Trainer can give the examples of any IP address starting with 10, or any IP address starting with “192.168”. Trainer should explain that these IP addresses can be used perfectly well on a local network, but not on the Internet. Trainer should explain that these IP addresses are used to make more efficient use of the available IP addresses in the following way:    1. Within the organisation, each PC is given an IP address that cannot be used on the Internet.    2. The organisation has a small number, perhaps just one, real Internet IP address assigned to it.    3. Whenever a PC wants to communicate with another computer on the Internet, the organisation’s infrastructure (Internet gateway router in particular) substitutes the real internet IP for the internal IP address before forwarding the traffic out to the Internet.    4. This allows a large number of PCs share a single IP address for communicating on the Internet, and the technique is known as Network Address Translation (NAT).   The upshot of the use of this technique, however, is that all of the PCs inside the organisation appear to the rest of the Internet as if they are a single computer with a single IP address. If this IP address is identified as part of an investigation, it is only the organisation itself that is in a position to determine which internal PC generated the traffic in question. | |
| **Slide 27** | Trainer should explain that one of the key sources of IP to subscriber identity information. The process for requesting such information from an Internet Service Provider will depend on national legislation, although some form of prosecutorial or court order is typically required. The period of time for which ISPs are required to retain records is also a matter for national legislation. A period of 2 years is common at the time of writing.  Which ISP owns the IP address in question: https://www.whoismyisp.org/ is a helpful resource in this regard.  The trainer should point out that the ISP may not be a national ISP in your country and therefore mutual legal assistance may be required to get access to this information. | |
| **Slide 28** | Trainer should point out that multinational service providers typically keep records of, for example, the IP address from which a particular account logged in. Trainer should explain that in cases where you are aware of a suspect, for example, Facebook account, it may be possible to find an IP address associated with the activity of this account from Facebook.  International cooperation, including cooperation with multinational ISPs is covered elsewhere in this course in more detail. | |
| **Slide 29** | Trainer should describe the scenario where an investigation points to an IP address owned by a company. Trainer should point out that in many cases companies use NAT to share a single internet IP address amongst all internal computers. In these cases, only the company is in a position to associate specific IP address usage with a particular internal PC. Therefore engagement with the company to assist with the investigation will be required.  How this engagement takes place will depend on national legislation.  Trainer should explain that this situation can be complicated by the fact that, even though records may exist, they might not exist within your country. If, for example, a company is part of a multinational organisation, they might not control or operate their own infrastructure. In a case like this, if records exist, they may be in another jurisdiction. Whether the company in your country are in a position to provide the records will depend on the organisational and technical structure. | |
| **Slide 31** | Trainer should explain that criminals may attempt to intentionally obfuscate their IP address, making it virtually impossible to identify their IP address.  Trainer should also explain that certain technologies, through their normal use and operation, might also make it virtually impossible to identify the suspect IP address. | |
| **Slide 32** | Trainer should explain that services exist online specifically to conceal the source of browsing and Internet activity. Trainer should show example webpage on next slide.  Trainer should point out that similar services are available to anonymise the source of email.  Trainer should explain that other services, such as TOR, the onion router, can be used to conceal source IP data. | |
| **Slide 34** | Trainer should explain that Carrier grade NAT is a serious problem for identifying a suspect associated with a particular IP address. The problem is that a second piece of information, known as a port number, is required to unambiguously associate a particular user with the IP address. In many cases, the port number is not stored in service records. Trainer should refer back to the web server logs and email headers and point out that no port number information is present in either of these sources.  Trainer note: See https://en.wikipedia.org/wiki/Carrier-grade\_NAT for useful background information. | |

|  |  |
| --- | --- |
| 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.  Trainer should talk through the objectives of each of the lessons from the first day and confirm the students’ understanding of the learning outcomes. This can be achieved, for example, through informal testing of the learning objectives of each lesson. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.2.2 – Electronic Evidence | | **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 * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Aim:** To provide the delegates with basic information about the use of electronic evidence in criminal proceedings. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Define electronic evidence * Explain the relevance of electronic evidence. * Explain how electronic evidence is identified, seized and handled. * Explain how electronic evidence is analysed. * List the relevant procedural provisions of the Budapest Convention. | | |
| **Introduction:**  This session provides information on the definition, handling and analysis of electronic evidence for use in criminal proceedings.  All information about this session is included in the PowerPoint presentation entitled “Session 1.2.2 – Electronic Evidence” 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. | | |
| **Slide Notes** |  | |
| **Slide 4** | The trainer should ask the students to give examples of what they think might be electronic evidence. The trainer should refer back to the proceeds-generating cybercrime examples provided in the cybercrime lesson (ransomware and banking malware, for example). Through guided discussion the trainer should identify the following categories of electronic evidence:   1. Dead box 2. Live data 3. Memory 4. Internet 5. Others such as mobile phone cell site analysis data   The trainer should then ask the participants to define evidence as per their national legislation. The trainer should ask does this definition apply to electronic evidence and discuss if not, why not. Trainer should ask if there is a specific definition for electronic evidence and what national legal provisions apply.  Trainer should ask the students what features of electronic evidence they can think of that might make electronic evidence special. This discussion will be carried forward to the next slide. | |
| **Slide 5** | Trainer should describe the nature of electronic evidence and discuss the volatility of the evidence, citing in particular the fact that it is very delicate in the sense that it is easily changed or deleted and also the fact that it is very transient and may not be available for a long period of time.  Reference could be made, for example, to IP addresses or other identifying characteristics associated with the activity of a malware. Alternatively, if the trainer considers that an example from the financial investigation realm would be more applicable at this point, the IP address associated with online banking or virtual currency activity might be appropriate. | |
| **Slide 6** | Trainer should continue discussion of the features of electronic evidence and discuss the fact that the evidence may be located outside of the jurisdiction and that this may raise a significant number of challenges. Additionally, the trainer should cite the (relatively simple) example of seizing a suspect’s PC.  Trainer should explain that a typical hard drive is at least 1 Terabyte in size, which is a huge amount of data to analyse. Trainer should also cite the example that the suspect PC may contain privileged communication. Therefore there are significant challenges due to the volume of evidence and the fact that the seized data may contain both evidential and non-evidential records.  Further, the trainer should explain that it might not be apparent in advance which sources of evidence will be relevant. Trainer can cite an example such as a child pornography investigation where the suspect keeps all data on USB keys rather than on the PC. A long time may be spent investigating the PC and no child porn will be found. Only when USB keys are investigated will the data be found. However, there is now an additional possible source of electronic evidence – proof on the suspect PC that the particular USB keys containing child porn were, in fact, used on that PC.  The trainer can also cite challenges such as the seizure of PCs which may contain evidence in a business context, but will also contain important business records that the company needs to continue operating. Seizure of large volumes of data, such as file servers, can present particular challenges.  Finally, the trainer should point out that in many cases, electronic evidence requires expert analysis and that this takes time and can introduce infrastructural bottlenecks. | |
| **Slide 8** | Trainer should talk through the examples of electronic evidence that are relevant in (a) cybercrime cases, (b) financial investigations and (c) other examples that might be applicable in virtually all types of crime. | |
| **Slide 9** | Trainer should make clear to the students that most investigators are not experienced with the handling of this type of evidence. However, certain groups of investigators are experienced, specifically cybercrime and/or digital forensic investigators. Trainer should point out that these investigators can support others (e.g. financial investigators) with guidance on the identification, analysis and interpretation of this type of evidence. | |
| **Slide 21** | Examples of forensic examinations  Within the four phases (and especially within the third phase) multiple forensic examinations are possible. The choice of the right investigation technique depends on various factors – in particular, the kind of offence that is in the focus of the investigation.  Among the most common techniques are the following:  Hardware analysis. If the investigators seize computer hardware then forensic experts can analyse the hardware to gather system-related information. Such an investigation can for example be relevant to prove whether the offender had the ability to connect a computer system to the Internet. Hardware analysis can in addition be relevant if – due to the transfer of system-related information during a registration process – it is known that the suspect used a specific hardware configuration.  Analysis of the function of computer software. Apart from the hardware, computer software plays an important role in the operation of a computer system. Forensic experts can for example determine the functions of computer virus or other form of malicious software. In addition they can reconstruct software operation processes. Furthermore, software analysis can be important to determine if the production or sale of software that can be used for legitimate as well as illegal purposes (dual-use) is criminalised.  Analysis of software installed on the suspect’s computer system. An analysis of the software installed on a computer system can provide the investigators with valuable information for further investigation. This is especially the case with regard to encryption software and tools used to securely delete files. If such software is installed on the suspect’s computer, further investigations can specifically address those issues.  Identification of relevant digital information. Computer data can be stored in different types of storage devices. And even within a hard disk there are various possibilities where a file can be saved. Identifying the storage location of relevant evidence is therefore challenging.  One of the new trends that presents additional challenges in identifying relevant digital information is the emerging use of remote storage. As highlighted above, the availability of broadband access and remote storage servers has influenced the way in which information is stored. By making use of such remote storage the suspect can prevent the seizure of the suspect’s computer hardware enabling the law enforcement agencies to access the information that is stored on the remote storage devices. Forensic analysis can in this case be used to verify if the suspect used remote storage services.  The identification of relevant digital information is not limited to files itself. Databases of software tools used by the suspect to find information on his computer might contain relevant information as well. Even system generated temporary files might contain evidence for criminal proceedings.  Identification of hidden files. Offenders can use techniques to hide files in a storage device in order to prevent law enforcement agencies from analysing the content of the file. This is especially relevant within investigations concerning illegal content. Forensic investigations can identify hidden files and make them accessible within the analysis.  Recovery of deleted files. If the offenders are using tools to ensure that files are securely deleting, recovery of this information is in general not possible. But in cases where the offenders are not aware of such tools, the deletion of digital information does not necessarily make them unavailable to law enforcement agencies as they can be recovered by using special forensic software tools.  Decrypting encrypted files and volumes and recovery of passwords. Criminals are more and more frequently using encryption technology. This technology creates significant challenges for law enforcement agencies as they are unable to access and examine the encrypted information. Within forensic analysis, approaches to decrypt encrypted files and storage devices can be undertaken. In addition, forensic experts can support law enforcement agencies to develop strategies to get access to encrypted files – for example, by using a key-logger.  Offenders are able not just to prevent access to certain information by using encryption, but also use password protection systems. Forensic analysis can use password recovery to enable law enforcement agencies to access password protection systems.  File analysis. Files stored on a storage device can be analysed in various ways. Forensic examinations can for example focus on the content of files. Apart from the manual examination of suspicious files, forensic investigations can include automatic keyword searches for text files and tools that automatically search for known images on the suspect’s computer.  As highlighted previously, computer data can be rather easily manipulated. Forensic examinations can prove alterations and the forgery of digital document.  Furthermore, investigations can take into account meta-data. These types of analyses can determine the time the document was last opened or modified. In addition, meta-data analysis can be used to identify the author of the file with a threatening message or the serial number of the camera that was use to produce child pornography image.  Authorship analysis. If threatening texts or hate speech are posted in blogs or forums on the Internet, the analysis of log-files might not lead the investigators to the author of the text if the suspect is acting from an Internet cafe or makes use of anonymous communication services. Sophisticated linguistic analysis can help to determine if the suspect wrote articles before and left information that can help to identify the individual in this context.  Maintaining the integrity of data. As pointed out previously, the protection of the integrity of digital evidence is crucial for the admissibility in court. Forensic experts can ensure the protection of the integrity of files during the collection of evidence. This enables law enforcement agencies in some cases to avoid the seizure of hardware and instead refer to copying the relevant files by protecting their integrity against any kind of alteration during the investigation process. This includes in particular the creation of images of storage media.  IP tracing. Offenders that use the Internet to commit crime (for example, downloading child pornography images or attacking computer systems) leave traces. Traffic data analysis, such as the examination of log-files kept by Internet servers, can lead the investigators to the connection used by the offender to log on to the Internet. Such investigations can be challenging if the offenders use anonymous communication technology. But even in those cases investigations are not impossible. One example is the forensic tool CIPAV (Computer and Internet Protocol Address Verifier) that was used in the US to identify a suspect using anonymous communication services.  E-mail analysis. E-mail has become a very popular form of communication and therefore plays an important role in computer forensics. Given that it is relatively easy to identify the sender of an e-mail with threatening message or illegal content attached, offenders very often use free e-mail addresses registered using fake personal information. Even in those cases, the examination of header information and log-files of the e-mail provider can in some cases enable an identification of the suspect.  Tracing financial transactions. A number of crimes - including the sale of child pornography – include financial transaction. By using data from commercial systems and institutions involved in the financial transactions it is possible to identify the offender. One example is an investigation in Germany where offenders who downloaded child pornography from a commercial website were identified by their credit card companies that analysed their customer records to identify customers that used their credit card to purchase child pornography on the specific website. Such investigations are more challenging if offenders make use of anonymous payment methods.  Real time collection of traffic data and the interception of content data. Forensic investigations can include the real-time monitoring of data transfer processed. This Council of Europe Project on Cybercrime www.coe.int/cybercrime enables the investigators to react to processes at the time the suspect of an investigation is acting.  Monitoring activities with regard to publicly available services. Publicly available services can be used to exchange copyright protected material or illegal content. Such services can within an investigation be monitored by forensic experts. This includes for example the observation of chat forums.  Remote forensics. Currently the need for remote forensic tools is discussed. This would enable live remote evidence collection and remote monitoring, without the suspect being aware of investigations on his system.  Carrying out such investigations requires specific training and well defined procedures that are based on widely accepted standards and methodologies. | |
| **Slide 25** | Article 14 of the Budapest Convention is proscribes the scope of the procedural rules. According to it, the Convention will be applicable – obviously - , when the crime under investigation is one of the listed crimes in the Convention, but it also, procedural rules can be used in the investigation of any crime if it was committed by the means of a computer system; second, the rules can also be applicable to the gathering of evidence in any investigation if the evidence, in the case, is stored in any kind of digital record: this means that every crime potentially falls under the procedural rules of the Budapest Convention.  There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law (many states limit the power of interception of oral communications or telecommunications to a range of serious offences, in recognition of privacy and the intrusiveness of this investigative measure). Second, a Party may reserve the right to apply measures in Article 20 (real-time collection of traffic data) only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted that the range of offences to which it applies the interception measure referred in Article 21 (some states consider collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness). | |
| **Slide 28** | Articles 16 and 17 describe expedited preservation of computer data and expedited preservation and disclosure of computer data. Both of the provisions are very innovative and extremely significant.  Traditional pieces of evidence will stay on the crime scene, eventually, for a long period of time, but digital data – electronic evidence -, once lost or destroyed, will be difficult to recover. Traffic data, for example, is very helpful to identify the perpetrator of a crime. But this type is information is not systematically available, unless it is implemented data retention legislation. Outside Europe, most counties did not yet implement such legislation. Thus, traffic data just can be obtained if there is a legal instrument allowing law enforcement agents to order the preservation of such volatile information.  The coexistence of the two provisions needs explanation, because they are different.  Concerning traffic data - just traffic data -, there is also a provision allowing expedited disclosure and not just preservation and storage. With respect to content data, this is not applicable: referring to this, it is just allowed the obligation of preservation - and not of disclosure -, until a proper order, issued by the competent authority is obtained. This restriction does not apply to traffic data, much less sensitive than other data. These rules, of course, must be considered in the framework of the domestic rules of communications secrecy, and Parties of the Convention can go further than the minimum levels described here.  In practical terms, this instruments is very useful in cases (most of them, in fact) where more than one service provide was involved in a communication – each one of them has the obligation to disclose the necessary information to identify the path of the communication. | |
| **Slide 30** | The provision of Article 18 is also very interesting. According to it, each Party must adopt legislative measures to empower its law enforcement authorities with the possibility of giving “production orders”. This judicial order can be issued by law enforcement agencies to citizens and to Internet service providers, ordering them to provide the competent authorities with data stored in a computer system, under their responsibilities or provide subscribers data.    According to the Convention, the production order must specify the nature and extent of the required data: it is very clear that the data required by the investigation must be previously determined; *fishing expeditions* are therefore prohibited. The purpose of this legal limit is to prevent abuse of these new investigative powers by law enforcement agents. In the real world, a search or seizure of objects or documents is normally only directed to objects or documents directly related to a case under investigation. In the digital world, if the rule was the complete permission of access to the whole information that comes with a piece of hardware, it would be permitted to access all kinds of information stored on that computer, often unrelated to the crime under investigation and (e.g. in the case of email communication) involving also third parties.    As it was already mentioned, Article 16 can create the obligation, to a service provider, to preserve data. Traffic data can be quickly disclosed, and transferred to law enforcement agencies. But, it was said, this provision of Article 17, just allows disclosure of traffic data.  Article 18, on its side, empowers the authorities to order the disclosure of any other type of information stored in a digital medium, pursuant or not a preservation order issue on the basis of Article 16. | |
| **Slide 32** | Search and seizure are described by Article 19 of Budapest Convention.  Most of national procedural rules include general regulations for search and seizure, but not all of them have specific rules governing computer search and computer seizure. Many jurisdictions can live well just with traditional searches and seizures. However, the real world teaches that digital investigations face challenges previously unknown caused, for example, by the interconnectedness of computer systems.  Enfacing that kind a new questions, Budapest Convention created specific rules to deal with searches and seizures in the digital world. For example, there is a specific rule, in Article 19, 2, relating to the hypothetic extension of a search when, during a search of a computer system, the investigators conclude that there is a need to extent that search to another computer system. Under the Convention, when an authority lawfully gains access to a specific computer system or part of it, and in the course of inspecting this system form a reasonable belief that the data sought is stored in another computer system in its territory, that authority can “expeditiously” extend the search to the other system.  Specifically with respect to seizures, there are some concrete topics that must be underlined because they are typical for the new digital environment: the various possibilities of physically seizing computer data.  As most of the legislations just have specific regulation to searches in the physical world, they don’t have special regulation to the new and more efficient ways that are available to seize computer data.  In particular, Budapest Convention demands that signatory states enact enabling legislation that allows during the process of a lawful seizure of computer data to:   * 1. seize physically a computer system,   2. make and retain a copy of those computer data (which is important in case the data is stored on a major server, where physical removal is impossible, and also when physical seizure would interfere too significantly with the rights of other people who have access rights to that machine – for instance the a big company’s server)   3. maintain the integrity of the relevant stored computer data and, finally, to   4. render inaccessible or remove those computer data in the accessed computer system.   This last provision is relevant for instance when physical seizure is impossible, but real harm could ensue if a third party got access of the data.  With the exception of the mere seizure of data in its own and original record, all these procedural possibilities are specific measures from the digital environment. | |
| **Slide 33** | Sometimes, the investigator needs more fresh information, rather than that information provided by the search or seizure of stored data. *Real-time* collection of computer data allows alive investigations and is described on Article 20 of Budapest Convention. Such a kind of intrusive measure requires proper legislation to allow law enforcement authorities to collect or record, through technical means, data in real time, and also the power to compel service providers to collect or record data from their costumers, within its normal activity, in real time.  This kind of investigative tool can be very important, for example, to establish the source of a communication, in view of identifying a perpetrator, in real time. | |
| **Slide 34** | Last, but not least Article 21 describes interception of content data. Besides of traffic data, sometimes, law enforcement authorities need to know the real content of communications between suspects of a crime. Some countries already have provisions on telephone interceptions, but not all of them allow the authorities to, specifically, intercept communications, other than by telephone.  That is the reason why, on Article 21, specifically, Budapest Convention includes provisions that enable investigators to intercept and record data communications.  Besides being a very powerful investigative tool, the interception of communications is also a very intrusive measure and is only allowed, by the terms of the Convention a range of serious offences to be determined by national laws.  Interception of content data is a very intrusive measure on private life, stringent safeguards are required to ensure an appropriate balance between the interests of justice and the fundamental rights of the individual. In the area of interception, the Budapest Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law. Nevertheless, the following important conditions and safeguards in this area, applied in domestic laws, are: judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality (e.g. legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; right of redress. Many of these safeguards reflect the European Convention on Human Rights. | |
| **Slide 35** | Trainer to add equivalent national procedural provisions here. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.2.3 – Online Criminal Money Flow Typologies (Part 1) | | **Duration: 120 Minutes** |
| **Resources required:**   * Laptop or PC running Windows 7, 8 or 10 and with Microsoft Office 2010 or later * Projector and display screen * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Aim:** The aim of this lesson (along with the other lessons on Online Criminal Money Flow Typologies) is to illustrate some of the most frequently used methods and instruments for (a) holding proceeds of online crime and (b) laundering proceeds from online crime. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the criminal money flow typology of the use of money remittance providers. * Explain the criminal money flow typology of the use of wire transfers, takeover/opening of accounts. * Explain the criminal money flow typology of the use of cash withdrawals. * Explain the criminal money flow typology of the use of Internet payment services. * Explain the criminal money flow typology of the use of money mules. * Explain the criminal money flow typology of the use of international transfers. * Explain the criminal money flow typology of the use of virtual currencies. * In the case of each typology listed above, list possible sources of evidence. * In the case of each typology listed above, list procedural powers in national legislation applicable to the identification of the use of the typology. * In the case of each typology listed above, and if applicable, list the procedural powers applicable to the freezing, seizing and confiscation of funds held in an online form. | | |
| **Introduction:**  This session provides information about a selection of online criminal money flow technologies.  All information about this session is included in the PowerPoint presentations entitled “1.2.3 – Online Criminal Money Flow Typologies (hour 1)” and “1.2.3 – Online Criminal Money Flow Typologies (hour 2)” 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. | | |
| **Slide Notes (Hour 1)** |  | |
| **Slide 4** | The trainer should ask the students what is a money remittance provider and to give examples of any specific money remittance providers they might be aware of. Examples that will typically arise are Western Union and MoneyGram.  Through guided discussion the trainer should identify the following categories of remittance providers:   * Large “traditional” providers, such as Western Union and MoneyGram * Informal value transfer networks and underground banking systems, such as Hawala networks   The trainer should ask the attendees how money remittance providers work, in general terms, focusing on the following key points:   1. Person A presents at a location of the remittance provider 2. They provide funds to the remittance provider 3. Person B presents at a location of the remittance provider (possible in a foreign jurisdiction) 4. Person B receives funds from the remittance provider 5. A fee is charged by the remittance provider for this service   The trainer should explain that most, but not all, money remittance providers have an online presence.  The trainer should highlight the point that there are both formal and informal money remittance providers. Formal examples are western union and MoneyGram. Informal remittance providers are common, often used within particular ethnic groups, whereby one individual will accept funds and transfer them to a family member in their home country. The family member in the home country will they pay out funds to the recipient in the home country. | |
| **Slide 5** | The trainer should ask the students what they consider to be the problems with money remittance providers from the perspective of investigation, search, seizure and confiscation of crime proceeds.  Through guided discussion the trainer should help the class to identify the following key issues:   1. If the remittance provider accepts or pays out in cash there is a possibility that an investigation could be impeded. 2. If the remittance provider does not adequately identify and retain identification of the customer, an investigation could be impeded. 3. If the remittance provider does not retain adequate transaction records, an investigation could be impeded. 4. If the remittance provider is not required by regulation to report suspicious activity, an investigation could be impeded. 5. If the remittance provider does not register their activities with the regulator, an investigation could be impeded. 6. The volume of legitimate cash transactions presents a challenge for identification of illegal cash transfers. | |
| **Slide 6** | Trainer should describe the typical remittance provider laundering typology, as per this slide.  Trainer should not focus too heavily on the mule recruitment aspect of the typology, because this will be covered separately elsewhere. | |
| **Slide 7** | Trainer should ask participants to discuss how they might approach an investigation where the money remittance provider itself, or some specific staff member, is complicit in the crime.  Trainer should also ask participants to discuss whether this is a higher risk in formal or informal money remittance providers. | |
| **Slide 8** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of remittance providers.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Remittance slips/receipts for funds 2. Forensic analysis of suspect computers can reveal use of online remittance services 3. Interviews with remittance provider staff 4. Records of remittance provider 5. Interception of suspect communication. | |
| **Slide 9** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of remittance providers.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 8). | |
| **Slide 12** | The trainer should ask the participants to consider a hypothetical scenario whereby a criminal has gained control of a victim’s bank account. The criminal would now like to extract funds from the victim’s bank account. What techniques can the criminal use to transfer/obfuscate the source of funds?  Through guided discussion the trainer should help the participants to identify the following key items:   1. International transfers 2. Structured transactions, using many small transactions below a reporting threshold 3. The use of mule accounts 4. The use of shell companies, either to transition or to aggregate funds 5. Withdrawing funds in cash 6. The use of compromised bank accounts as mule accounts 7. The use of payment services to purchase goods online   Trainer should not focus too heavily on the mule recruitment aspect of the typology, because this will be covered separately elsewhere.  Trainer should not focus too heavily on the cash withdrawal aspect of the typology, because this will be covered separately elsewhere. | |
| **Slide 13** | Trainer should describe the typical wire transfer laundering typology, as per this slide.  Trainer should not focus too heavily on the mule recruitment aspect of the typology, because this will be covered separately elsewhere. | |
| **Slide 14** | Financial institutions are heavily dependent on online banking services but that the non-face-to-face nature of the online banking service presents additional risks. It is also reasonable for a financial institution to expect that a certain percentage of customers will fall victim to cybercrime attacks and lose control of their banking credentials. The trainer should ask the participants to consider what controls financial institutions put in place to prevent the misuse of the banking credentials of a victim who has lost control of their banking credentials.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Additional controls around creation of new beneficiaries and international transfers (e.g. a customer may be allowed to log in to view their balance but may need to call a call-centre in order to set up a new beneficiary). 2. The use of second authentication factors, such as two factor authentication devices, mobile SMS codes, etc. 3. Automated fraud detection techniques which will identify transactions that are out-of-character for a particular customer | |
| **Slide 15** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of wire transfers.  Through guided discussion the trainer should help the participants to identify the following key items:   * Banking records of the victim’s financial institution * Additional/new beneficiaries added to victim’s bank account * Forensic analysis of suspect PCs can reveal the use of online banking services * Large numbers of transfers of funds with descriptions such as “gift”. | |
| **Slide 16** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of wire transfers.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 15). | |
| **Slide 18** | The trainer should ask the students to discuss what challenges they think cash might present to cybercriminals, as opposed to other types of crime.  Through guided discussion, the trainer should help the students to identify the following key points:   1. Due to the inherently trans-national nature of cybercrime, cash withdrawn in one country may not easily be transferrable into the possession of the organising criminals, who may be residing in a different country. Therefore, further transfers, at additional cost to the criminals, will be required. 2. Direct contact is required between criminals to hand over cash. 3. Direct contact is required, in many cases, to use cash value. 4. Cybercriminals frequently structure funds into many small transactions to avoid financial reporting requirements and therefore aggregating the cash can be logistically challenging. 5. Carrying large amounts of cash across border increases risk of seizure 6. Cybercriminals are not stealing cash directly and therefore the cash is predominantly of value as a technique for breaking the chain of value. | |
| **Slide 20** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of cash withdrawals.  Through guided discussion the trainer should help the participants to identify traditional indicators of cash usage, such as possession of large volumes of unexplained cash. Also, technological indicators such as possession of large numbers of prepaid value cards. | |
| **Slide 21** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of cash withdrawals.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 20). | |
| **Slide 23** | The trainer should ask the students what is a Internet payment service and to give examples of any specific Internet payment services they might be aware of. The example that will typically arise is Paypal.  Through guided discussion the trainer should identify the following categories of Internet payment services:   1. Banks offering money transfer services, where the Internet is only the channel through which the payment instruction is issued. 2. Non-banking services, operating only on the Internet, which are indirectly associated with a bank account.   The trainer should ask the attendees to consider what is the significance of banks offering money transfer services where the Internet is the channel through which the payment instruction is issued. Through guided discussion the trainer should help the attendees identify that the non-face-to-face nature of the transaction is the key differentiator. | |
| **Slide 25** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of Internet Payment Services.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Banking records of the victim’s financial institution 2. Additional/new beneficiaries added to victim’s bank account 3. Forensic analysis of suspect PCs can reveal the use of online banking/Internet payment services 4. Records of Internet payment service provider. | |
| **Slide 26** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of Internet payment services.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 25). | |
| **Slide 27** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held by an Internet payment service provider.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| **Slide Notes (HOUR 2)** |  | |
| **Slide 4** | Trainer should describe explain that mules are essential to many online laundering schemes.  Broadly speaking there are two categories of mules; those that know they are participating in illegal activity and those that think they are involved in a legitimate activity, e.g. a job offer.  Trainer should explain that unwilling mules are recruited through job offers listed on legitimate recruitment websites for jobs such as “financial manager” or “work at home” positions. Spamming services are also used to advertise and recruit potential money mules. | |
| **Slide 5** | The trainer should ask the students to discuss the issue of willing vs. unwilling mules. The trainer should guide the discussion as follows:  The unwilling mule is often described as a credulous individual who is deceived by the professional nature of the engagement by their “employer” and believes that they are working for a legitimate company. However, this image is now being questioned more and more by police because there have been numerous instances where it has become apparent that the mule was fully aware of the illegal nature of their deeds.  The trainer should ask the opinion of the participants and consider how one might go about establishing whether or not an individual that is claiming to be an unwilling mule was, in fact, unaware of the illegal nature of their activities. | |
| **Slide 6** | Trainer should describe the typical money mule laundering typology, as per this slide. | |
| **Slide 7** | The trainer should ask the students to discuss the issue value of arresting/charging mules. The trainer should guide the discussion as follows:  The amount of funds handled by any particular mule is usually small, typically totalling less than 3,000 USD. However, when the amount of funds handled through the entire mule network is aggregated, the gains for the organisers of the cybercriminal activity are substantial, of the order of millions of dollars. The trainer should ask the students to bear in mind that the organisers of the cybercriminal activity may be located in more than one foreign jurisdiction, the organised crime activity can be complex and time consuming.  The trainer should also point out that a common technique involving money mules is for the mules to enter the country for the specific purpose of money mule activity. If they are arrested, it will presumably be their first offence in this jurisdiction and therefore they will, most commonly be charged and released, at which point the mule flees the country.  The trainer should ask the students to discuss the value of charging individual mules. The trainer should also ask the students to consider if and how the international organised criminal activity should be approached. | |
| **Slide 8** | The trainer should ask the students what they consider to be the problems with money remittance providers from the perspective of investigation, search, seizure and confiscation of crime proceeds.  Through guided discussion the trainer should help the class to identify the following key issues:   1. If the remittance provider accepts or pays out in cash there is a possibility that an investigation could be impeded. 2. If the remittance provider does not adequately identify and retain identification of the customer, an investigation could be impeded. 3. If the remittance provider does not retain adequate transaction records, an investigation could be impeded. 4. If the remittance provider is not required by regulation to report suspicious activity, an investigation could be impeded. 5. If the remittance provider does not register their activities with the regulator, an investigation could be impeded. 6. The volume of legitimate cash transactions presents a challenge for identification of illegal cash transfers. | |
| **Slide 9** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the activity of money mules.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Suspicious transaction reports from financial institutions where mules have accounts/presented themselves 2. Records from financial institution where stolen funds where held 3. Mule’s financial records. | |
| **Slide 10** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/activity of money mules.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 9). | |
| **Slide 11** | Note: During the discussion of international transfers, the trainer should endeavour to keep the conversation away from the area of international cooperation mechanisms, because this is covered in a separate lesson later in the day. | |
| **Slide 13** | The trainer should ask the participants to consider challenges arise to the search, seizure and confiscation of criminal funds when the funds have been transferred internationally.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Increased difficulty gaining access to evidence 2. Mutual legal assistance delays 3. Jurisdictional issues 4. Inconsistent regulation of financial entities (e.g. virtual currency exchanges) 5. *Broken audit trails. How can you follow the criminal money trail if the funds are removed in cash?* | |
| **Slide 14** | Trainer should describe the typical international transfer typology, as per this slide. | |
| **Slide 15** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of international transfers.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Suspicious transaction reports made by financial entities to FIU 2. Banking records of the victim’s financial institution 3. Additional/new beneficiaries added to victim’s bank account 4. Forensic analysis of suspect PCs can reveal the use of online banking services. 5. *Admissions* 6. *Special Investigative techniques* 7. *Surveillance*. | |
| **Slide 16** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of international transfers.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 15). | |
| **Slide 18** | The trainer should ask the students to identify any virtual currencies they are aware of.  Through guided discussion, the trainer should help the students to identify at least the following:   * One example of a decentralised virtual currency, such as bitcoin * One example of a centralised virtual currency such as linden dollars * One example of e-money such as google checkout, paypal, payment cards, etc.   Any ideas identified by the students should be written on a flipchart, whiteboard etc. | |
| **Slide 19** | Trainer should explain that this course uses FATF definitions for virtual currency, e-money and digital currency. See for further information:  [http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf%20)  Trainer might like to reference the ECJ judgement C-264/14 of October 22nd 2015, where the following definition is used:  “49. Transactions involving non-traditional currencies, that is to say, currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to the transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions.  52. In the case in the main proceedings, it is common ground that the ‘bitcoin’ virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators.  55. It is common ground that the ‘bitcoin’ virtual currency is neither a security conferring a property right nor a security of a comparable nature.”  The trainer should guide the students through a whiteboard exercise where the digital currencies identified during the previous discussion should now be categorised using the terminology here. | |
| **Slide 20** | The trainer should, referring to the previous slide, point out that all three definitions refer to a “digital representation”. The trainer asks the participants what they think the significance of this expression in the definitions. The trainer should explain that this is an important point with significant practical and legal implications for cases involving digital currency.  Through guided discussion, the trainer should help the students to identify the following key points:   1. A digital representation is a representation of something in the form of digital data. 2. A physical object such as a computer, flash drive, CD ROM etc. may contain a digital representation of currency but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the relevant virtual currency system. 3. The critical point is that the digital data itself is the virtual currency, not the medium on which the digital data is stored. 4. The digital data can be copied or transferred to another storage medium, but the value remains inherent in the digital representation. | |
| **Slide 21** | Trainer should explain that this course uses FATF definitions for virtual currency, e-money and digital currency. See for further information:  <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.  The trainer should guide the students through a whiteboard exercise where the digital currencies identified during the previous discussion should now be categorised using the terminology here. | |
| **Slide 22** | Trainer should briefly introduce Bitcoin, being one of the most popular virtual currencies, particularly with cybercriminals. | |
| **Slide 23** | Trainer should highlight some of the key properties of Bitcoin. | |
| **Slide 24** | Trainer should explain using the example of ransomware, how criminals use virtual currencies. | |
| **Slide 25** | Trainer should explain the virtual currency ecosystem concepts on this slide:  Virtual Currency Exchange: A person or entity engaged in the business of exchanging virtual currency for real currency, funds, other virtual currencies, precious metals, etc. for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wire transfers, credit cards and other virtual currencies. The currency exchange(s) may or may not be associated with the virtual currency administrator.  Virtual Currency Administrator: A person or entity engaged as a business in issuing (putting into circulation) or redeeming (withdrawing from circulation) a virtual currency. A virtual currency administrator will only exist for centralised virtual currencies. By definition, a decentralised virtual currency does not have an administrator.  A user/owner is a person who obtains virtual currency and uses it to purchase goods or services or transfers it to another person.  A miner is a person who participates in the operation of decentralised virtual currency by running software on their computer(s) to solve complex mathematical problems. The operation of mining is essential to the functioning of decentralised virtual currencies, such as Bitcoin, because the solution to the complex mathematical problem solved by the miners serves as the basis for validation of transactions in the virtual currency system. Miners typically receive a reward in virtual currency for performing mining activity.  A virtual currency wallet is a software, or other mechanism, for holding, storing and transferring virtual currency.  A wallet provider is an entity that provides a virtual currency wallet service to hold, store and transfer virtual currency. The wallet provider holds a user’s private keys, possession of which allows the user to conduct transactions involving specific currency units. Wallet providers provide services such as backups (hot or cold backups), mixing (obfuscation of virtual currency transactions), etc.  Merchants receive funds in the form of virtual currency from users/owners in exchange for goods and services.  Other entities such as software developers, site administrators and so on may also be involved in the operation of a virtual currency. | |
| **Slide 26** | The trainer should ask the participants to consider how the virtual currency ecosystem interfaces with the traditional financial system.  Through guided discussion the trainer should help the participants to identify the following interfaces:   1. Virtual currency exchanges 2. Financial institutions 3. Cash/ATMs 4. Payment Cards 5. Money remittance providers 6. Merchants accepting virtual currency. | |
| **Slide 27** | Trainer might want to point out that the 4th EU money laundering directive will require customer due diligence to be carried out by virtual currency exchanges. | |
| **Slide 28** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of Virtual Currencies.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Banking records of the victim’s financial institution 2. Forensic analysis of suspect PCs can reveal the use of virtual currency software and/or virtual currency exchange 3. Examination of blockchain/transaction records of virtual currency provider 4. Records of virtual currency exchange 5. Records of virtual currency administrator (if exists).   Trainer should ask participants to consider what types of information might be available from a virtual currency business. Virtual currency businesses that are subject to know-your-customer (KYC) obligations would be able to provide:   * Identity documentation (which could include user’s picture) * Location verification documentation * IP address * Phone number * Transaction history * Deposit and withdrawal addresses * Bank name, bank account number and transaction information. | |
| **Slide 29** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of cash withdrawals.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 25). | |
| **Slide 30** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held in the form of virtual currency.  Through guided discussion the trainer should help the participants to identify the relevant national provisions.  Depending on the student group, the trainer may consider highlighting some of the challenges with freezing, seizing and confiscation of virtual currency value, such as volatility of the exchange rate, the fact that the criminal may have wallet backups stored elsewhere, etc.  These topics are further elaborated in the advanced course. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.2.4 – Online Criminal Money Flow Typologies (Part 2) | | **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 * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Aim:** The aim of this lesson (along with the other lessons on Online Criminal Money Flow Typologies) is to illustrate some of the most frequently used methods and instruments for (a) holding proceeds of online crime and (b) laundering proceeds from online crime. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the criminal money flow typology of the use of purchasing through the Internet. * Explain the criminal money flow typology of the use of shell companies. * Explain the criminal money flow typology of the use of prepaid cards. * Explain the criminal money flow typology of the use of online gaming and online trading platforms. * In the case of each typology listed above, list possible sources of evidence. * In the case of each typology listed above, list procedural powers in national legislation applicable to the identification of the use of the typology. * In the case of each typology listed above, and if applicable, list the procedural powers applicable to the freezing, seizing and confiscation of funds held in an online form. | | |
| **Introduction:**  This session provides information about a selection of online criminal money flow technologies.  All information about this session is included in the PowerPoint presentations entitled “1.2.4 – Online Criminal Money Flow Typologies (hour 3)” 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. | | |
| **Slide Notes (Hour 1)** |  | |
| **Slide 4** | The trainer should ask the students to discuss the issue of purchases through the internet. The trainer should guide the discussion as follows:   * Suppose you had a stolen credit card, how could you use it on the Internet for your personal gain? * The trainer should highlight the following key points: * Purchasing goods and services through the Internet, which are then shipped to the criminal or to a mule, is a good way of converting stolen data into real-world value. * Goods and services which can be easily resold are particularly attractive. One particular example (other than obvious things like jewellery and other high-value goods) is airline tickets. * The use of stolen data is prevalent in high-risk markets such as counterfeit pharmaceuticals, firearms, child pornography, etc. * Online gambling sites are another high-risk area for money laundering/use of stolen credentials * The use of online auction sites is another risk area. | |
| **Slide 5** | Trainer should describe the typical internet purchase typology as per this slide. Trainer should point out that the financial advantage to the criminal comes from the payment from the winner of the auction, not directly from the compromised credentials. With this in mind, the trainer should ask the students what difference it makes if the payment comes via the action site (e.g. ebay), via an Internet payment service (e.g. paypal) or directly from the winner (e.g. by bank transfer or money remittance provider). | |
| **Slide 6** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of Internet purchases.  Through guided discussion the trainer should help the participants to identify the following key items:   * Records of the Internet site where the purchase transaction was performed (e.g. auction site) * Records of the payment mechanisms used to pay for the purchased goods (e.g. paypal) * Possession of goods * Records of service provider if service paid for using stolen credentials * Electronic evidence on suspect PC indicating use of internet payment services and/or internet purchase sites. | |
| **Slide 7** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/activity of Internet purchases.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| **Slide 8** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held in the form of virtual currency.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slides 7 and 8). | |
| **Slide 12** | The trainer should ask the participants to consider challenges arise from the use of shell companies, particularly in the case where online crime proceeds are involved.  Through guided discussion the trainer should help the participants to identify the following key items:   * Increased difficulty gaining access to evidence * Mutual legal assistance delays * Jurisdictional issues * Increased complexity of financial/money laundering scheme may present challenges for online service providers. | |
| **Slide 13** | Trainer should describe the typical shell company typology, as per this slide. | |
| **Slide 14** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of shell companies.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Suspicious transaction reports made by financial entities to FIU 2. Banking records of the victim’s financial institution 3. Additional/new beneficiaries added to victim’s bank account 4. Forensic analysis of suspect PCs can reveal the use of online banking services 5. Business activities, assets and liabilities (or lack thereof) of shell company 6. Owners/controllers of shell company 7. Legal structure of shell company. | |
| **Slide 15** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of shell companies.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 14). | |
| **Slide 16** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds held by a shell company.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| **Slide 20** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of prepaid cards.  Through guided discussion the trainer should help the participants to identify the following key items:   * The possession of prepaid cards (or mobile phone topups, or other forms of anonymous credit) * Forensic analysis of suspect PCs can reveal the activity of purchasing prepaid cards and/or selling prepaid cards * Evidence from the physical location where the prepaid cards were purchased. | |
| **Slide 21** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of prepaid cards.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |
| **Slide 22** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of prepaid cards.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 21). | |
| **Slide 23** | Note that the focus of this presentation is on the risks presented by online gaming platforms[[17]](#footnote-17).  Trainer should explain that the risks presented by online gaming platforms are understood, they have not been well studied at the time of writing of this course. Therefore, the information in this section is based on anecdotal experience and an understanding of the risks presented by these platforms at the time of writing. | |
| **Slide 24** | Trainer should explain that online betting platforms allow for gambling of various types, from poker to scratch cards, horse racing, sports betting, etc.  Trainer should explain that funds are typically lodged to an account held by the online betting platform, from which bets are placed and to which winnings are lodged. Funds can be lodged using a variety of techniques although typically bank transfers and payment cards are used. Trainer should reference the prepaid cards discussion from immediately before this section.  Players can typically have their winnings credited to a bank account or to a payment card.  Trainer should point out that there are challenges with regulation of online gambling, due to the fact that in some countries online gambling platforms are illegal, whereas in others they are not. Additionally, due to the trans-national nature of the Internet, online gambling companies are often not in the jurisdiction where the players are located. | |
| **Slide 26** | The trainer should ask the participants to consider what sources of evidence might be available to indicate the use of online gambling platforms.  Through guided discussion the trainer should help the participants to identify the following key items:   1. Records of online gambling company 2. Suspicious activity reports by online gambling company, if online gambling company is regulated in your jurisdiction and required to produce suspicious activity reports. 3. Forensic analysis of suspect PCs can reveal the use of online gambling platforms (web activity and/or installed software). | |
| **Slide 27** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the identification/use of online gambling platforms.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. Through discussion, the trainer should help the students to identify the provisions within national legislation that allow for the identification and collection of evidence of the types identified above (in the discussion on slide 26). | |
| **Slide 28** | The trainer should ask the participants to consider, based on the possible sources of evidence identified in the previous discussion, what procedural powers are available in their national legislation to allow for the freezing, seizing and confiscation of funds from online gambling platforms.  Through guided discussion the trainer should help the participants to identify the relevant national provisions. | |

|  |  |  |
| --- | --- | --- |
| Lesson: 1.2.5 – International Cooperation Methodologies | | **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 * Whiteboard, flipchart or other technique for recording student input * These resources are only needed if the trainer is using a PowerPoint presentation | | |
| **Aim:** To provide the delegates with information about international cooperation in financial and cybercrime investigations. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Explain the relevance of international cooperation in targeting online crime proceeds. * Explain the advantages of combining international cooperation avenues in the field of cybercrime and electronic evidence as well as, financial investigation and money laundering. * Distinguish international cooperation on exchange of information and on mutual legal assistance. * Enumerate relevant international networks and organisations for exchange of information. * Describe the nature, purpose and process of mutual legal assistance (MLA) * Present relevant international legal instruments * Identify relevant provisions of the Budapest and Warsaw conventions in order to be able to use them appropriately. | | |
| **Introduction:**  This session provides information about international cooperation methodologies in financial and cybercrime investigations.  All information about this session is included in the PowerPoint presentations entitled “1.2.5 – International Cooperation” 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. | | |
| **Slide Notes** |  | |
| **Slide 3** | Cybercrime and online crime is often trans-border in nature and therefore international cooperation is crucial. Networks and organisations to facilitate the **exchange of information** are developed in the field of cybercrime (such as the 24/7 network and Europol EC3), financial investigations (CARIN) and money laundering prevention and investigation (EGMONT Group). INTERPOL should also be mentioned. Traditional **mutual legal assistance** is necessary for the execution of court orders to gather evidence, and to freeze and confiscate property abroad, even if it might take a lot of time. Alternative approaches might also be useful, such as Joint Investigation Teams (JITs) or conducting parallel investigations.  Online crime specifics  The Internet, notwithstanding its many positive aspects, provides opportunities for abuse by criminals who can act in almost invisible ways, rapidly and anonymously, to conceal their identity (for example by using Darknet services), evidence and traces of criminal profits. This characteristic of the Internet represents a challenge for law enforcement agencies.  In cases involving computers, or the Internet, **being used as a tool or an object of a crime**, the perpetrator does not need to be physically on the territory of a jurisdiction. Neither does any of the evidence necessarily need to be within the territory of a jurisdiction. By using the Internet, the perpetrator can operate in one country, using servers located in another country, to target a victim in a third country, while the proceeds of crime end up in a fourth country. The Internet knows no borders, but borders still exist for police and prosecutors. International cooperation for the purpose of investigation and evidence gathering is therefore essential. | |
| **Slide 4** | Criminal investigations have to answer questions like: who is behind a particular IP address while that IP address was being used to communicate with a victim or another criminal? To establish the counterparts in a criminal activity, it might be important to analyse the traffic or even the content of communication that is stored by a company with headquarters abroad. Also when conducting financial investigations and analysing money flows, it is important to have access to bank account data and transactions abroad, and the possibility to postpone the transaction (FIU) or to freeze the transaction (court order), or property, for example in a bitcoin wallet.  Facing such practical challenges, it is important to understand what are the legal and practical possibilities to request and receive assistance in the form of information or evidence from a particular country. Success in concrete cases often depends on established contacts, mutual interest and trust.  **Combining 3 aspects**  The concept of targeting online crime proceeds brings together the approaches of **cybercrime investigation, financial investigation and money laundering investigation** with the purpose of increased efficiency and success of criminal investigations and criminal proceedings from the perspectives of both prosecuting a criminal and targeting and confiscating the proceeds of crime.  It is important to recognise the benefits of combining different possibilities for international cooperation by combining the three aspects. It should be noted however, that despite the possible efficient tools to prevent and combat money laundering, in several countries the prosecution of money laundering is still a challenge.  In cases of online crime investigation the speed is essential. When elements of the money laundering offence exist (criminal proceeds are being disguised or concealed) the FIU can use its power to access bank data and postpone the suspicious bank transaction and moreover, to request this measure from an FIU abroad. A subsequent court order to access bank data and/or freeze transaction abroad and MLA will be needed. | |
| **Slide 5** | Law enforcement (police and prosecutors) cooperation and **exchange of information** is indispensible in cross-border investigations. Relevant networks play an important role in this respect.  **Mutual legal assistance** is still considered as the principal means to enforce court orders and to gather evidence abroad. The length of this formal procedure often represents an important obstacle. The use of joint investigations and JITs might address some of the challenges of efficiency.  **International legal instruments**, such as the Budapest and Warsaw conventions, provide for legal obligations to assist another party to the Convention. International cooperation in concrete cases is more efficient when mutual interest exists. It is therefore important to build professional relations with counterparts abroad. The international networks of experts offer opportunities to exchange best practice and build trust. Some international networks are created also to exchange operational information. Personal data protection rules apply in such cases. As the financial investigation should be conducted in parallel to the cybercrime (and online crime) investigation, it is useful to identify the relevant networks in the areas of cybercrime and e-evidence, as well as in the areas of targeting proceeds of crime (financial investigation) and prevention/investigation of money laundering.  In the investigation of criminal offences committed by international criminal groups, it is necessary to verify whether the offenders have any property abroad. In such cases, police or prosecutor international cooperation is very important. A contact person in a foreign police force can advise as to what data on property can be obtained from public sources, through police cooperation or by a letter rogatory. Such information can make the acquisition of data considerably easier and faster.  Note that such cooperation is operational and execution of court orders is excluded. The networks to facilitate the cooperation have been established. Even if these channels cannot be used for formal mutual legal assistance, the conditions for mutual legal assistance and other practical advice can be shared through these channels. Such cooperation can also lead to establishment of joint investigation teams, which in principle can facilitate also more effective mutual legal assistance approaches. It can also lead to arrangements of parallel investigations in cross border cases with more perpetrators and victims. | |
| **Slide 6** | Who can help?  **Camden Asset Recovery Interagency Network (CARIN)**  <http://carin-network.org/>  CARIN is an informal network of experts/practitioners in the field of asset tracing, freezing and confiscation. Europol is a permanent secretariat of CARIN. Exchange the best practice and information on legal possibilities in the area of targeting proceeds of crime. The operational information between the two contact points can be exchanged bilaterally.  **The Egmont Group**  <https://egmontgroup.org/en>  Egmont Group is a body of 152 Financial Intelligence Units (FIUs). The Egmont Group is a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). It is used to exchange the operational information in a concrete case between FIUs. The network of FIUs is used to exchange information on STRs, bank data and to temporarily postpone financial transactions on the basis of a request by an FIU (see Warsaw Convention, Chapter V, Articles 46 and 47).  **24/7 Network of the Budapest Convention** for exchange of information and assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (See Budapest Convention, Article 35).  **INTERPOL, Europol (EC3 for cybercrime) or Eurojust** are channels for police and prosecutors.  For South-eastern European countries:  *Also other regional and bilateral contacts of police and prosecutors are of great importance, such as the Southeast European Law Enforcement Centre (SELEC) or Police Cooperation Convention for Southeast Europe (PCCSEE).*  **Southeast European Law Enforcement Centre (SELEC)**  <http://www.selec.org/>  The objective of SELEC, within the framework of cooperation among competent authorities, is to provide support for member states and enhance coordination in preventing and combating crime, including serious and organised crime, where such crime involves or appears to involve an element of trans-border activity.  **Police Cooperation Convention for Southeast Europe (PCCSEE)** provides the legal framework for police cooperation and exchange of information.  <http://www.pccseesecretariat.si/>  The Committee of Council of Europe experts – MONEVVAL and Conference of the Parties to the CETS 198 in the area of money laundering and terrorist financing, cybercrime (T-CY) or cooperation in criminal matters (PC-OC) besides their respective tasks, also provide for opportunities for experts to establish working contacts.  Trainer should explain that, whilst not being avenues for international cooperation, the following relevant bodies are carrying out relevant work in this area and it might be useful to follow their reports/plenaries:   * Committee of experts on the evaluation of anti-money laundering measures and the financing of terrorism (MONEYVAL), <http://www.coe.int/t/dghl/monitoring/moneyval/>   Conference of the Parties to the CETS 198 (monitoring mechanism based on Warsaw Convention),  <http://www.coe.int/t/dghl/monitoring/cop198/about/about_en.asp>   * The Cybercrime Convention Committee (T-CY), <http://www.coe.int/en/web/cybercrime/tcy> * Committee of experts on the operation of European Convention on cooperation in criminal matters (PC-OC), <http://www.coe.int/t/DGHL/STANDARDSETTING/PC-OC/> * The Financial Action Task Force (FATF), <http://www.fatf-gafi.org/>   The FATF is an inter-governmental body. The objectives of the FATF are to set standards and promote implementation of legal, regulatory and operational measures for combatting money laundering, terrorist financing and other related threats to the integrity of the international financial system.  **Mutual legal assistance** is formal cooperation and the result of a request can be used as evidence in court. Usual channels of communications are through the designated central authorities, often Ministries of Justice. The possible channels can also be the Ministry of Foreign Affairs or through the Interpol channel in urgent cases.  Note that within the EU mutual legal assistance is running directly between responsible authorities (prosecutor/court). Warsaw (Article 34) and Budapest (Article 27/29) conventions also provide for such approach in urgent cases, with formal requests transmitted through the central authorities as well.  The receiving state is obliged to recognize or execute the request for cooperation or court order.  National legislation regulates the forms of international cooperation, including mutual legal assistance, while it is based on relevant international legal instruments. In the area of targeting online crime proceeds the Council of Europe Convention on money laundering, search, seizure and confiscation of crime proceeds and terrorist financing (Warsaw Convention) and Budapest Convention on Cybercrime are the key ones.  Usually the content of a request (legal conditions and justification), the language and the communication channel is defined in the law. If no international agreement with certain third country exists, cooperation would be possible on the basis of the principle of reciprocity.  **Identify relevant national legislation that defines conditions for international cooperation (legislation on police and prosecution office) and mutual legal assistance (legislation on criminal procedure/international cooperation).** | |
|  |  | |
|  |  | |
| **Slide 7** | International cooperation can be described from a procedural and institutional perspective (who does what). Also the relevant international networks are added to illustrate the different avenues.  In cases of cybercrime and online crime investigations cross-border cooperation is driven by the needs of the domestic investigation and the available timeframe. For example, in case of CEO fraud as explained in the section on cybercrime, the police or prosecutor’s contact person abroad might provide advice on legal conditions in the third country and on the most effective approach to MLA. Depending on the conditions provided in the national legislation, the police can propose to the prosecutor to request the court order to be  executed abroad related to a request for house search, interrogation, and access to bank data, freezing order, seizure of electronic evidence, including to disclose traffic or content data related to electronic communication.  Mutual legal assistance is needed also for the execution of freezing or confiscation orders, if the property is abroad. However, management of frozen property, costs of management, disposal and sharing of confiscated assets usually require practical arrangements and agreement between the two parties.  Provisions on transfer of proceedings in criminal matters, extradition and transfer of sentenced persons are also defined by national and international legal instruments.  The judge who is issuing the court order, according to the national legislation, should also take into account the requirements related to mutual legal assistance requests, on the basis of a specific convention or practice in cooperation with the third country. The central authority for international cooperation, usually the Ministry of Justice, might be able to provide necessary advice.  There is an obligation to execute requests that meet the requirements, but the efficiency and speed depends also on direct bilateral contact and trust. In the area of e-evidence a voluntary and direct cooperation with internet service providers (ISPs) is very important, when allowed by domestic legislation. Particularly this is the case for multinational service providers (Facebook, Google, Microsoft, etc.) based in the USA, that allows for timely preservation of data until a mutual legal assistance request is transmitted and to sharing information on subscribers, taking into account domestic legislation of the requesting state.  Since the mutual legal assistance process to gather evidence or to execute court requests, in practice, might take a long time, that the investigators in reality do not have, alternative forms of cooperation are being promoted, such as joint investigation teams (JITs) or parallel investigations. In a case of mutual interest and intensive involvement, the responsible authorities of two countries tend to act and react in a timely fashion. | |
| **Slide 8** | The relevant conventions such as the Council of Europe Warsaw and Budapest conventions as well as European Convention on mutual assistance in criminal matters and additional protocols provide for legal obligation and avenues and options for exchange of information and execution of court orders in cross border cases.  The trainer should recall that cooperation with Parties to the preceding 1990 Strasbourg Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime is regulated in Article 49, paragraph 6 of Warsaw Convention.  Also UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) of 1988 and the UN Convention Against Transnational Organised Crime (Palermo Convention) of 2001 are relevant in this area.  Also bilateral agreements on mutual legal assistance in criminal matters and police cooperation agreements must be relevant in this respect.  International legal instruments contain aspects of criminalisation of conduct, procedural powers (investigation tools) and international cooperation, including legal basis for mutual legal assistance (MLA).  The fields of freezing and confiscation of proceeds of crime and money laundering (Warsaw Convention) and cybercrime (Budapest Convention) will be addressed from the perspective of international cooperation and mutual legal assistance. They provide for avenues that can be used and combined in order to achieve most effective results when conducting parallel financial and (cyber)crime investigation.  The Warsaw Convention sets up the central authorities for investigative, freezing and confiscation and mutual legal assistance. In emergency situations, direct cooperation between responsible judicial and prosecution authorities is foreseen (Article 34) as well as the direct cooperation between Financial Intelligence Units (FIUs), including administrative postponement of transactions.  The Budapest Convention provides for 24/7 network for cooperation (at police and/or prosecutor level) and allows also for requests for the preservation of data and the collection of evidence.  Also the traditional Convention on mutual legal assistance in criminal matters with its protocols can be used. | |
| **Slide 9** | Relevant provisions for international cooperation available under the Warsaw and Budapest conventions will be presented to allow the identification of appropriate possibilities when combining cybercrime investigation, financial investigation and money laundering (prevention and) investigation. Cooperation applies subject to national provisions and with safeguards for postponement or refusal of request (Warsaw Convention, Section 5, Article 27 and Budapest Convention, Article 25/4 and 27/4 and 5). Article 24 of the Budapest Convention also regulates extradition. | |
| **Slide 10-14** | **General principles and measures for international co-operation**  (Warsaw C., Article 15)  The Parties shall mutually co-operate for the purposes of investigations and proceedings aiming at the confiscation of instrumentalities and proceeds. Party shall comply with requests for confiscation of specific items or requirement to pay a sum of money corresponding to the value of proceeds and for investigative assistance and provisional measures with a view to either form of confiscation.  (Budapest C., Article 23 and 25)  The Parties shall afford mutual assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.  **Investigative assistance**  (Warsaw C., Articles 16 – 20) Parties shall assist in the identification and tracing of instrumentalities and proceeds, which includes securing evidence as to the existence, location or movement, nature, legal status or value of the aforementioned property. Such assistance comprises also of Requests for information on bank accounts, on banking transactions and monitoring of banking transactions and spontaneous information.  (Budapest C., Articles 31-34): Mutual assistance regarding investigative powers: Accessing of stored computer data; Trans-border access to stored computer data with consent or where publicly available; Mutual assistance regarding the real-time collection of traffic data, Mutual assistance regarding the interception of content data.  **Spontaneous information**  (Warsaw C., Article 20) and (Budapest C., Article 26): Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. (2...)  **Provisional measures**  (Warsaw C., Articles 21-22):Parties shall take the provisional measures, such as freezing or seizing, to prevent any dealing in, transfer or disposal of property and provide spontaneously all information relevant for provisional measure.  (Budapest C., Articles 29-30): following measures are foreseen: Expedited preservation of stored computer data, Expedited disclosure of preserved traffic data.  **Confiscation** (Warsaw C.) Parties are requested either to enforce a confiscation order or to submit the request to its competent authorities for the purpose of obtaining an order of confiscation and enforce it. This includes request to pay a sum of money corresponding to the value of proceeds, or confiscation of specific item of property (Article 23). Paragraph 5 of Article 23 provides for execution of a judicial request for measures equivalent to confiscation leading to the deprivation of property, which are not criminal sanctions (non conviction based confiscation).  Article 25 determines the **rules of assets sharing**: property is primarily disposed of by executing Party, unless requested to give priority consideration to returning it to the requesting Party so that it can give compensation to the victims or return property to their legitimate owners.  **Exemption on Direct communication**  (Warsaw C., Article 34) In the event of urgency, under Article 34/2, requests may be sent directly between the judicial authorities, including prosecutors, with a copy to be sent through central authorities. Under Article 34/3 a request or communication may be made through the (Interpol). Under Article 34/5 the non coercive requests may be directly transmitted between the competent authorities. Under Article 34/6 direct exchange of draft request is possible.  (Budapest C., Article 27/9) provides for similar provision in case of urgency.  **24/7 network**  (Budapest C., Article 35): Each Party shall designate a point of contact available on 24/7 basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: the provision of technical advice; the preservation of data pursuant to Articles 29 and 30; the collection of evidence, the provision of legal information, and locating of suspects.  **FIU cooperation**  (Warsaw C., Chapter V, Articles 46 and 47): FIUs exchange, spontaneously or on request and either in accordance with this Convention or in accordance with existing or future memoranda of understanding compatible with this Convention, **any accessible information** that may be relevant to the **processing or analysis of information** or, if appropriate, to in**vestigati**on by the FIU regarding **financial transactions** related to money laundering and the natural or legal persons involved. Article 47: FIU **postponement of suspicious transactions.** | |
| **Slide 15** | Trainer should discuss with students:   * Who is national central authority for Warsaw and Cybercrime convention? * Who is the contact point for CARIN, EGMONT Group and 24/7 network? * Do you have an ARO established? * Who is national member of the Conference of the Parties to the CETS 198, MONEYVAL and T-CY?   National legislation on:   * JITs, parallel investigation, * Mutual legal assistance. | |
| **Slide 16** | Trainer should discuss with students:   * Which domestic authorities are involved in international cooperation: exchange of information, MLA and postponement of transaction? * Relevant networks and organisations? Who are the national contact points? * Who is the central authority for Warsaw and Budapest convention? * Which information can be requested and which procedural requests can be made on the basis of Warsaw and Budapest convention? * What is the relevant domestic legislation for international cooperation (police, prosecutors, MLA)? * What is the practice with direct ISP cooperation in the USA? * Data on MLA/STATISTICS (incoming/outgoing)? * Number of cross border financial investigation and exchange of info * Number of MLA requests bank data orders (in/out) * Number of MLA requests for freezing/confiscation orders (in/out) * Number of MLA requests in cybercrime cases, MLA for subscriber, traffic and content data, e-evidence. | |
| **Slide 17** | Exercise  Discuss domestic legal provisions and jurisprudence on:   * MLA request and execution: * Access to bank data * Access to ISP subscriber, traffic and content data, including interception * Preservation request directly to ISP * Access, seizure and forensic analysis of stored computer data (e-evidence) * Freezing of transaction/property * Confiscation of property * Asset sharing   Provide/discuss templates/forms for:   * MLA request on the basis of national legislation in relation to Budapest and Warsaw conventions * Expedited preservation of stored computer data and disclosure of traffic data * Direct preservation request to ISP * Request through 24/7 network (Budapest convention) * FIU request to postpone financial transaction abroad. | |

|  |  |
| --- | --- |
| Lesson: 1.2.6 – 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 on-going minor modification or during a scheduled major modification update. | |
| **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.

1. Appendix 1

**Legal Instruments: Council of Europe, United Nations and the European Union**

* Convention on Laundering, Search, Seizure And Confiscation of the Proceeds From Crime, Strasbourg, ETS 141, 8.11.1990.
* Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.5.2005.
* Convention on Cybercrime, ETS 185, 23.11.2001.
* Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189, 28.01.2003.
* United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances, Vienna, 19.12.1988. (Article 5).
* United Nations Convention Against Transnational Organized Crime, New York, 15.11.2000. (Articles 12-14).
* United Nations Convention Against Corruption, New York, 31.10.2003. (Articles 31, 54-57).
* Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union (OJ L 127/39, 29.4.2014, p. 39–50).
* Directive 2013/40/EU on attacks against information system calls on Member States to ensure that they have an operational national point of contact in the existing 24/7 cooperation networks and
* Directive 2014/41/EU on the European Investigation Order in criminal matters, which aims to make cross-border investigations across the EU faster and more efficient on the basis of mutual recognition.
* Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003, p. 45).
* Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2006, p. 59).
* Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (L 332/103, 18.12.2007, p. 103-105). For example, introduced the obligation to establish Asset Recovery Office(s) (ARO).
* Joint Action 98/699/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, Seizing and confiscation of instrumentalities and the proceeds from crime (OJ L 333, 9.12.1998, p. 1).
* Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001, p. 1).
* Council Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property (OJ L 68, 15.3.2005, p. 49).
* Proposal for a Directive amending Directive (EU) 2015/849 on thepreventionoftheuseofthefinancialsystemforthepurposeofmoneylaunderingorterroristfinancingandamendingDirective 2009/101/EC, aimed at regulating virtual currencies by obliging providers of exchange, COM (2016) 450 final, 5.7.2016.
* Conclusions on improving criminal justice in cyberspace and Conclusions on the European Judicial Cybercrime Network[[18]](#footnote-18) (June 2016, Council of the European Union) (European Judicial Cybercrime Network).

**Evaluation of the Practical Application of International Instruments for International Cooperation**

* EU[[19]](#footnote-19) GENVAL 2012 Final report on the fifth round of mutual evaluations - "Financial crime and financial investigations"[[20]](#footnote-20)
* The 7th round of EU mutual evaluations (GENVAL)[[21]](#footnote-21) is devoted to the practical implementation and operation of the European policies on prevention and combating cybercrime.
* The Council of Europe’s Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC) 2014 questionnaire[[22]](#footnote-22)
* The Council of Europe Cybercrime Convention Committee T-CY:
* T-CY Assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime (2014)[[23]](#footnote-23).
* T-CY Recommendations to make the MLA process regarding cybercrime and electronic evidence more efficient (2014)[[24]](#footnote-24).
* T-CY Emergency requests: Preliminary observations on replies (2016)[[25]](#footnote-25)
* T-CY(2016)5 Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY[[26]](#footnote-26)
* T-CY(2015)16 Draft Guidance Note on Production Orders (Article 18) - Version of May, September and November 2016 (16th T-CY Plenary)
* T-CY(2016)2 Criminal justice access to data in the cloud: cooperation with foreign service providers
* T-CY(2016)7 Criminal justice access to electronic evidence in the cloud – Informal summary of issues and options under consideration by the Cloud Evidence Group
* T-CY(2015)10 Criminal justice access to data in the cloud: challenges
* T-CY(2016)13 Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers: Compilation of replies.

**European Court of Human Rights Case-law**

* Compilation of relevant case-law on personal data protection available at: <http://www.echr.coe.int/Documents/FS_Data_ENG.pdf>
* Compilation of relevant case-law on new technologies: <http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf>
* Compilation of relevant case-law on mass surveillance: <http://echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf>

**European Court of Justice Case-law**

* IP addresses may qualify as “personal data” under EU privacy law
* http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974
* Virtual currencies
* http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=160800

**Other**

* Europol2016 Internet Organised Crime Threat Assessment (IOCTA) 2016, available at:

[https://www.europol.europa.eu/activities-services/main-reports/internet-organised- crime-threat- assessment-iocta- 2016](https://www.europol.europa.eu/activities-services/main-reports/internet-organised-%20crime-threat-%20assessment-iocta-%202016)

* European Union SeriousandOrganised Crime Threat Assessment 2017, available at:

<https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>

* FATF's Best practices on confiscations 2012, available at:

<http://www.fatf-gafi.org/media/fatf/documents/reports/Best%20Practices%20on%20%20Confiscation%20and%20a%20Framework%20for%20Ongoing%20Work%20on%20Asset%20Recovery.pdf>

**Networks**

* Camden Assets Recovery Interagency Network(CARIN)
  + <http://carin-network.org/>
* The Egmont Group
  + <https://egmontgroup.org/en>
* 24/7 Network of the Budapest Convention
  + <https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%207%20567%2024-7%20text%20ets_en.pdf>
* Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
  + <http://www.coe.int/t/dghl/monitoring/moneyval/>
* The Cybercrime Convention Committee (T-CY)
  + <http://www.coe.int/en/web/cybercrime/tcy>
* Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters (PC-OC)
  + <http://www.coe.int/t/DGHL/STANDARDSETTING/PC-OC/>
* The Financial Action Task Force (FATF)
  + <http://www.fatf-gafi.org/>
* Police Cooperation Convention for Southeast Europe
  + <http://www.pccseesecretariat.si/>
* Southeast European Law Enforcement Centre (SELEC)
  + <http://www.selec.org/>

1. The European Union/Council of Europe Joint Project CyberCrime@IPA, Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime aimed at strengthening the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime. [↑](#footnote-ref-1)
2. The European Union and Council of Europe Joint Project “Targeting crime proceeds on the internet in South Eastern Europe and Turkey” – iPROCEEDS aims at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet. [↑](#footnote-ref-2)
3. Explanatory memorandum to the Proposal for an EU directive on countering money laundering by criminal law (22.12.2016) [↑](#footnote-ref-3)
4. Criminal Money Flows on the Internet – methods, trends and multi-stakeholder counteraction, MONEYVAL research report, March 2012, available here: http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6\_Reptyp\_flows\_en.pdf [↑](#footnote-ref-4)
5. At global level, according to United Nations estimates, the total amount of criminal proceeds in 2009 was approximately USD 2.1 trillion, or 3.6% of global GDP. The size of proceeds from criminal activity in the main illicit markets in the European Union for which evidence is available, has been estimated to amount to EUR110 billion. The amount of money currently being recovered in the EU is only a small proportion of the estimated criminal proceeds (Explanatory memorandum tot the Proposal for an EU directive on countering money laundering by criminal law (22.12.2016)). [↑](#footnote-ref-5)
6. MONEYVAL research report, Criminal money flows on the Internet, methods, trends and multi-stakeholder counteraction, March 2012. [↑](#footnote-ref-6)
7. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p.8). [↑](#footnote-ref-7)
8. FATF (2012), Interpretative Note to Recommendation 30, 2nd paragraph.

   See also: FATF (2012) Report Operational issues- Financial Investigation Guidance. [↑](#footnote-ref-8)
9. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.05.2005. [↑](#footnote-ref-9)
10. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, ETS 141, 8.11.1990. [↑](#footnote-ref-10)
11. See Europol: 2016 Internet Organised Crime Threat Assessment (IOCTA):

    <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> [↑](#footnote-ref-11)
12. The Proposal for a Directive amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directive 2009/101/EC is aiming at regulating virtual currencies by obliging providers of exchange services and custodial wallet providers to cooperate with FIU. [↑](#footnote-ref-12)
13. See European Court of Justice Judgment C-264/14, October 22nd 2015. [↑](#footnote-ref-13)
14. Normally the effort should be made to discover the bank accounts of the suspect during the investigation. If this is not successful, it is an international standard that information on bank accounts of a criminal has to be provided (see art. 7 and 17. of the Warsaw Convention and Chapters 2.3 and 2.5.1). In some countries the court practice does not allow for such circular query at the moment. [↑](#footnote-ref-14)
15. If the legislation allows extended confiscation of proceeds with a reversed burden of proof, additional elements are defined on the basis of which it can be deduced that the offender's property exceeding legally reported property within a certain period results from criminal offences. [↑](#footnote-ref-15)
16. FATF and national FIUs publish money laundering typologies. See FATF website at <http://www.fatf-gafi.org/publications/?hf=10&b=0&q=typologies&s=desc(fatf_releasedate)> [↑](#footnote-ref-16)
17. FATF (2009) Report on Vulnerabilities of Casinos and Gaming Sector, see

    <http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf> [↑](#footnote-ref-17)
18. <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>. [↑](#footnote-ref-18)
19. See also: <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/financial-investigation/index_en.htm> [↑](#footnote-ref-19)
20. <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202> [↑](#footnote-ref-20)
21. Adopted reports can be found at: <http://www.coe.int/da/web/octopus/blog/-/blogs/genval-evalutation-reports-on-cybercrime> [↑](#footnote-ref-21)
22. Questionnaire on the use and efficiency of Council of Europe instruments as regards international co-operation in the field of seizure and confiscation of proceeds of crime, including the management of confiscated goods and asset sharing. PC-OC Mod (2015) 06Rev4, 19.5.2016. [↑](#footnote-ref-22)
23. T-CY(2013)17rev, 3 December 2014, http://www.coe.int/en/web/cybercrime/t-cy-reports. [↑](#footnote-ref-23)
24. See page 125 to 127 of the report at<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c> [↑](#footnote-ref-24)
25. T-CY(2016)13, 25.7.2016,[Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers: Compilation of replies](http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ab6ab). [↑](#footnote-ref-25)
26. T-CY (2016)5, 16 September 2016:<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e> [↑](#footnote-ref-26)